Fusion Centers:

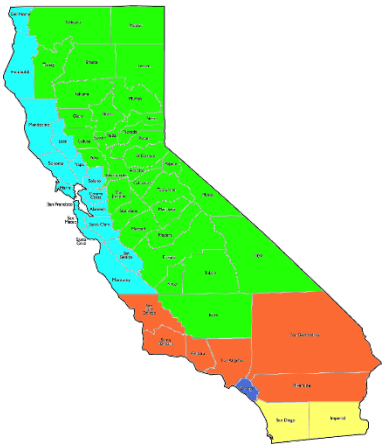
Social Media, Blue Leaks, & Suspicious Activity Reporting

2 Views – ACLU versus NSA

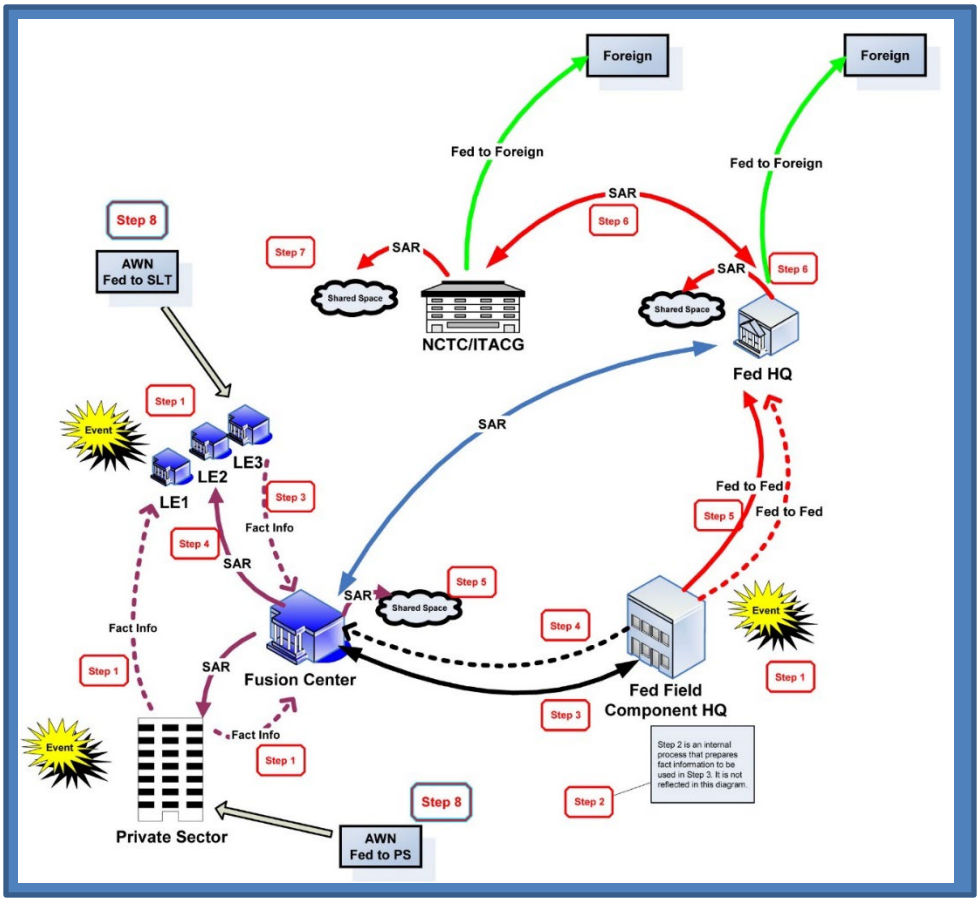
Where there is collection of data, there is always the prospect of great use and/or bad abuse.

And, much of the data culled has been packaged and delivered directly from the individual user, via social posts about getting vaccinated, vacation plans, new purchases, 10 year challenge photos (assisting in AI facial recognition), attendance at protests, and check-ins at every restaurant, workout, and airport - complete with selfies, food photos, and Fitbit results.

The Orange County Intelligence Assessment Center (OCIAC) monitors, stores, and analyzes massive amounts of internet communications including social media. Recent data analysis led OCIAC to identify seven members of The Base, a violent neo-Nazi white supremacist group, resulting in arrests in four states on charges including conspiracy to murder a Barstow couple and plans to overthrow the US government.



After 9/11, intelligence hubs were created to share anti-terrorism intelligence between local, state, and federal law enforcement agencies. The scope of these 80 fusion centers, each created independently, has expanded in scope to "detecting, deterring, disrupting, preventing, and mitigating the impact of drug activity, active shooters, transnational organized crime, cybercrimes, acts of terrorism, and other manmade and natural disasters" and are designed to "continuously collect data."



Fusion centers gained attention recently after Black Lives Matters protests. A massive data leak, called "the Blue Leaks", of over a million files of highly sensitive FBI, law enforcement, and fusion center files, was published online, including 24 years of data stolen from 251 law enforcement websites. The data showed close monitoring of protests and BLM organizers. In Milwaukee, protestors identified from videos posted on social media received tickets in the mail for breaking curfew during the protests. Inspector Formolo explained that any social medial information accessed by Milwaukee's Virtual Investigations Unit (VIU) is all open-source material, "Our guys are just pretty good at knowing how to go about connecting dots and stuff. That why we call it 'social network analysis.'"

The Blue Leaks include personal information for police officers, such as name, rank, agency, email, home address, and cell phone number. Some files include ACH routing numbers, international bank account numbers, and other financial data. There are reasonable concerns that individual officers could be harmed as a result of the data breach.

Ilia Lolochenko, Founder and CEO of ImmuniWeb security company, expressed his concerns regarding publication of this largest hack of US law enforcement agencies, "The eventual outcome of this leak will likely have disastrous effects for many innocent people. First, it will likely inflict irreparable reputational, financial and even physical harm to suspects and people charged with crimes who later were acquitted in a court of law."

Fusion Centers are owned and operated by state and local entities with support from federal partners in the form of training, security clearances, and Homeland Security grants. In early 2012, the Foreign Intelligence Surveillance Court approved sharing raw NSA data with the National Counterterrorism Center (NCTC) which oversees the intelligence community, including the Department of Homeland Security, FBI, and federal fusion center partners.

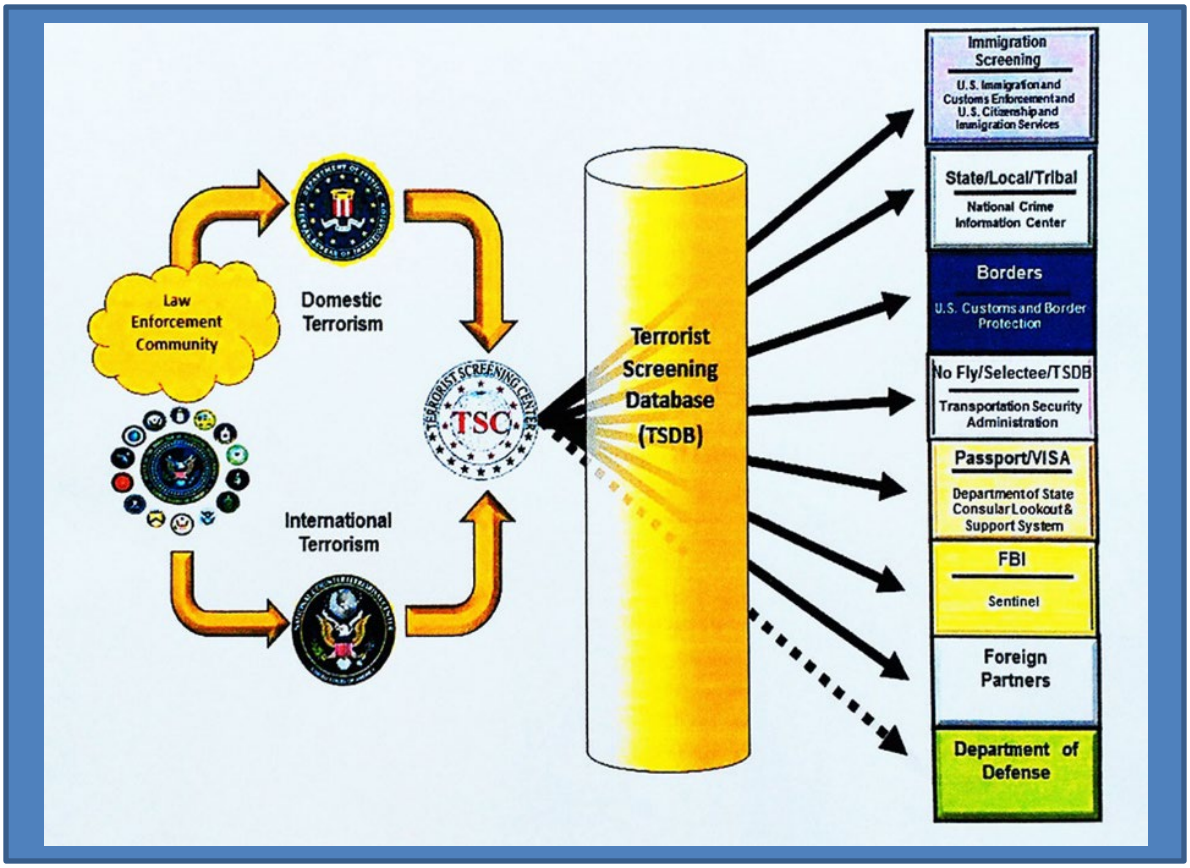
Excerpt, 3 Ways to Improve Fusion Center Intelligence for Local Agencies:

"Data has a shelf life and must remain complete and timely. Incomplete data sets can cause certain criminal activities to be underrepresented, which can lead to law enforcement agencies either over- or underestimating threats and ineffectively allocating resources. Data must also be fresh and relevant; agencies can't afford to rely on outdated information, especially when dealing with rapidly unfolding events. Yet keeping data for historical learning and longitudinal studies its also important."

Gretchen Stewart, Chief Data Scientist, Intel Public Sector
Juan Colon, Advisory Industry Consultant, SAS Institute

The ACLU has expressed concerns that “[t]here appears to be at least some conscious effort to circumvent public oversight by obscuring who is really in charge of these fusion centers and what laws apply to them” finding that federal authorities reap the benefits of working with the centers but avoid responsibility. And, because some state have stronger privacy or open-records laws than the federal government, fusion centers can manipulate who owns the records or where they are officially held to avoid stricter privacy protections. “Since no two fusion centers are alike, it is difficult to make generalized statements about them. Clearly not all fusion centers are engaging in improper intelligence activities and not all fusion center operations raise civil liverties or privacy concerns. But some do, and the lack of a proper legal framework to regulate their activities is troublesome.”

The National Security Agency (NSA) has strategic partnerships with 80 global corporations including AT&T, DXC, HP, Qwest, Motorola, Cisco, Qualcomm, IBM, Oracle, Intel, Microsoft, and Verizon to provide hardware, network infrastructure, application software, and operating system support. The NSA collects data from internet searches, websites visited, emails sent/received, social media activity, blogging, videos watched and/or uploaded, photos viewed and/or uploaded, cell phone apps and GPS, phone call records, text messages, Skype calls, online purchases, credit card transactions, financial information, legal documents, travel documents, health records, cable shows watched and/or recorded, commuter toll roads, electronic bus and subway passes, Smart passes, facial recognition data from surveillance cameras, educational records, arrest records, driver’s license, and DNA.



Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), led by the US Department of Justice, Department of Homeland Security, FBI, and state and local law enforcement agencies, collects and processes fusion center data including from tips provided by citizens. These tips are used to initiate investigations. The reportable behaviors listed in the National SAR standards include taking photos of buildings “in a manner that would arouse suspicion in a reasonable person.” The problem may lie in the fact that some people are more reasonable than others.

SAR reporting has had great success in financial crimes including bank fraud and money laundering. In one case, investigators were able to uncover a fraudulent investment scheme in southern California that robbed hundreds of investors, mostly Filipino immigrants, of over $25M. Alternatively, some of reported activities include middle eastern males purchasing pallets of water and Chinese nationals taking photos of the Folsom Dam. Notably, there have been numerous cases reported of people reporting criminal activity against blacks, where video and witness testimony clearly demonstrate otherwise, including a woman trying to prevent a black man from entering his own condominium.

The ACLU concerns about fusion centers center around privacy, racial and ethnic profiling, and SAR abuses. In the view of the NSA, “If you have nothing to hide, you have nothing to fear.” The truth probably lies somewhere in between the two. But, bottom line, at least this time, you cannot blame it entirely on Mark Zuckerberg.

Karen Heumann, COO

G2M, a re-grate-it, inc. brand