COMPUTERWORLD

# Cops run unauthorized searches on confidential databases for revenge, stalking

*Cops run unauthorized searches on confidential law enforcement databases for revenge, stalking, curiosity and to sell the information to others, an Associated Press investigation found.*

Darlene Storm

September 28, 2016

If a person intentionally gained "unauthorized access" to a computer or system, then he or she could be prosecuted under the Computer Fraud and Abuse Act (CFAA). Yet if a cop does more or less the same thing by running unauthorized searches in confidential law enforcement databases, it's likely no one would know about the misuse of the system nevertheless prosecute the police officer.

And some officers do run searches that have nothing to do with their jobs, claiming they are legally authorized to access the database, even though such searches have been used to help a rogue cop stalk a lover, for revenge against journalists, or to try to get even with some other enemy.

The Associated Press wanted to find out how often cops do abuse their power by misusing law enforcement databases packed with sensitive and personal information about citizens. After the investigation, the Associated Press revealed, "No single agency tracks how often the abuse happens nationwide, and record-keeping inconsistencies make it impossible to know how many violations occur."

However, by requesting records from state agencies, police departments and the FBI, the AP said some systems were "exploited by officers who, motivated by romantic quarrels, personal conflicts or voyeuristic curiosity, sidestep policies and sometimes the law by snooping. In the most egregious cases, officers have used information to stalk or harass, or have tampered with or sold records they obtained."

325 times between 2013 and 2015, cops and employees who misused databases "were fired, suspended or resigned." More than 250 times, the abusers were reprimanded, received counseling or a lesser form of discipline. There were another 90 cases in which it was unclear what discipline – if any – was handed out. AP said to keep in mind that "the number of violations was surely far higher since records provided were spotty at best, and many cases go unnoticed."

There's no tracking how often information obtained via the FBI's "National Crime and Information Center, a searchable clearinghouse that processes an average of 14 million daily transactions," is misused. There are audits every three years, but the feds rely on local agencies to address NCIC violations.

AP did find that confidential law enforcement databases were misused by:

- A cop who wanted a hospital employee's number after she caught his eye.
- A Phoenix cop traded investigation details with a woman for sex.
- A cop accepted a bribe to run a search on a woman's license plate number in order to discover if she was an undercover cop.
- A jealous marshal wanted the license plate number run for every white pickup truck because his girlfriend was allegedly stepping out on him with a dude who drove such a truck.

You may recall that some NSA employees pulled the same types of jealous-snooping stunts, except they tapped into the agency's surveillance power toeavesdrop on love interests, aka LOVEINT, or track email addresses of an ex.

The Associated Press said one cop sold NCIC data to a private investigator for defense attorneys. In August, the Ninth Circuit Court overturned a CFAA conviction for employee misuse of a sensitive database. The case involved an investigative agency which bribed a cop to access police databases and hand over the information.

Other officers ran unauthorized searches for relatives. Searches were run as a form of payback after a citizen questioned a sheriff's programs and spending; that time, unauthorized searches were conducted about the woman, her husband and daughter.

Sometimes police officers ran searches simply because they were curious about someone; for example, one admitted to checking on "dozens of officers and celebrities including basketball star LeBron James."

One cop, dubbed the "cannibal cop" by the media, ran searches on people who wrote nasty things about him. AP said he argued in court that "he was legally authorized to access the database."

"A lot of people have complicated personal lives and very strong passions," said Jay Stanley, a senior policy analyst with the ACLU Speech, Privacy, and Technology Project. He told AP, "There's greed, there's lust, there's all the deadly sins. And often, accessing information is a way for people to act on those human emotions."

In the end, the Associated Press investigation found, "Police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work."

There’s not any hard rules for how to handle such misuse. Although officers are prosecuted sometimes, it is “rarely at the federal level.” AP explained, “It's unsettled whether improper database access is necessarily a federal crime and whether it violates a trespass statute that criminalizes using a computer for other than authorized purposes.”

While the full Associated Press report goes into more detail about the investigation and results, the Cato Institute also keeps an eye on such misconduct via the National Police Misconduct Reporting Project.