Peekaboo, I See You: Government Authority Intended for Terrorism is Used for Other Purposes

The Patriot Act continues to wreak its havoc on civil liberties. Section 213 was included in the Patriot Act over the protests of privacy advocates and granted law enforcement the power to conduct a search while delaying notice to the suspect of the search. Known as a "sneak and peek" warrant, law enforcement was adamant Section 213 was needed to protect against terrorism. But the latest government report detailing the numbers of "sneak and peek" warrants reveals that out of a total of over 11,000 sneak and peek requests, only 51 were used for terrorism. Yet again, terrorism concerns appear to be trampling our civil liberties.

Throughout the Patriot Act debate the Department of Justice urged Congress to pass Section 213 because it needed the sneak and peak power to help investigate and prosecute terrorism crimes "without tipping off terrorists." In 2005, FBI Director Robert Mueller continued the same exact talking point, emphasizing sneak and peek warrants were "an invaluable tool in the war on terror and our efforts to combat serious criminal conduct."

A closer look at the number of sneak and peek warrants issued (a reporting requirement imposed by Congress) shows this is simply not the case. The last publicly available report about sneak and peek warrants was released in 2010; however, the Administrative Office of the US Courts has finally released reports from 2011, 2012, and 2013.

What do the reports reveal? Two things: 1) there has been an enormous increase in the use of sneak and peek warrants and 2) they are rarely used for terrorism cases.

First, the numbers: Law enforcement made 47 sneak-and-peek searches nationwide from September 2001 to April 2003. The 2010 report reveals 3,970 total requests were processed. Within three years that number jumped to 11,129. That's an increase of over 7,000 requests. Exactly what privacy advocates argued in 2001 is happening: sneak and peak warrants are not just being used in exceptional circumstances—which was their original intent—but as an everyday investigative tool.

Second, the uses: Out of the 3,970 total requests from October 1, 2009 to September 30, 2010, 3,034 were for narcotics cases and only 37 for terrorism cases (about .9%). Since then, the numbers get worse. The 2011 report reveals a total of 6,775 requests. 5,093 were used for drugs, while only 31 (or .5%) were used for terrorism cases. The 2012 report follows a similar pattern: Only .6%, or 58 requests, dealt with terrorism cases. The 2013 report confirms the incredibly low numbers. Out of 11,129 reports only 51, or .5%, of requests were used for terrorism. The majority of requests were overwhelmingly for narcotics cases, which tapped out at 9,401 requests.

Section 213 may be less known than Section 215 of the Patriot Act (the clause the government is currently using to collect your phone records), but it's just as important. The Supreme Court ruled in *Wilson v. Arkansas* and *Richards v. Wisconsin* that the Fourth Amendment requires police to generally "knock and announce" their entry into property as a means of notifying a homeowner of a search. The idea was to give the owner an opportunity to assert their Fourth Amendment rights. The court also explained that the rule could give way in situations where evidence was under threat of destruction or there were concerns for officer safety. Section 213 codified this practice into statute, taking delayed notice from a relatively rare occurrence into standard operating law enforcement procedure.

The numbers vindicate privacy advocates who urged Congress to shelve Section 213 during the Patriot Act debates. Proponents of Section 213 claimed sneak and peek warrants were needed to protect against terrorism. But just like we've seen elsewhere, these claims are false. The government will continue to argue for more surveillance authorities—like the need to update the Communications Assistance to Law Enforcement Act—under the guise of terrorism. But before we engage in any updates, the public must be convinced such updates are needed and won't be used for non-terrorist purposes that chip away at our civil liberties.

Discover more. Join our email list for EFF news, events, campaigns, and ways to support digital freedom.

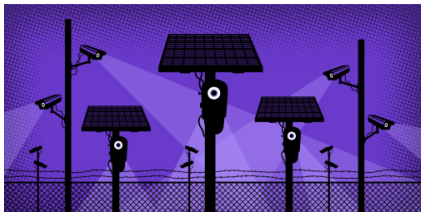
POSTAL CODE (OPTIONAL)

EMAIL ADDRESS *

SIGN UP NOW

I would like to join EFF's email list for EFF news, events, campaigns, and ways to support digital freedom.

RELATED UPDATES



DEEPLINKS BLOG BY KAREN GULLO, ADAM SCHWARTZ | SEPTEMBER 9, 2026

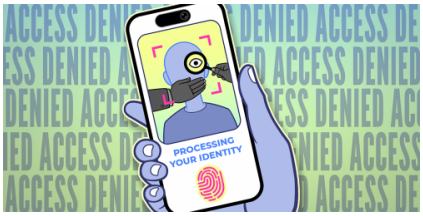
Cops Play Hide and Seek About Using Spy Tech to Avoid Scrutiny and Bad PR

Law enforcement agencies across the country are increasingly relying on spying technologies—automated license plate readers (ALPR), cell-site simulators, and facial recognition, to name a few--causing an outcry in many communities where people are rightly concerned about the threat to civil rights and civil liberties these tools present.Some...

Digital Sovereignty: What It Is, What It Could Be

DEEPLINKS BLOG BY JILLIAN C. YORK, EVA GALPERIN | SEPTEMBER 9, 2026

The term “digital sovereignty” has become ubiquitous. European officials invoke it in debates about cloud infrastructure, AI, semiconductors, and platform regulation. Governments throughout the global majority use it to argue for greater control over data and communications infrastructure and boost their economies. Companies market “sovereign cloud”...



DEEPLINKS BLOG BY DAVID GREENE | SEPTEMBER 1, 2026

Meta's $17 Billion Settlement is a Bad Deal for Teens and All Social Media Users

Meta’s settlement with 52 state attorneys general is a bad deal for all internet users, and especially for teens. In this post, we go through the Settlement’s provisions in detail.

DEEPLINKS BLOG BY DALY BARNETT | AUGUST 31, 2026

Doxxing Safety Part II: Incident Response

Doxxing, also known as the deliberate sharing of personal information to harass or endanger someone, is a tricky thing to protect against. It often happens by some ill-intentioned person accessing publicly available information, then sharing that information more widely in the hopes it will intimidate their target or worse. This...

DEEPLINKS BLOG BY DALY BARNETT | AUGUST 31, 2026

Doxxing Safety Pt I: Prevention and Footprint Management

Doxxing is the deliberate disclosure of personal information in order to bully, harass, intimidate, or instigate a chain of harms against someone. It's a tricky thing to protect against when the jerk doing it is often able to use legal and accessible means to do so. The odds are stacked...

DEEPLINKS BLOG BY VERIDIANA ALIMONTI | AUGUST 27, 2026

EFF and Allies on Brazil's Elections: Privacy Protections are Crucial to Electoral Integrity

EFF, Access Now, and Data Privacy Brasil are putting forward recommendations to strengthen robust privacy and data protection safeguards in the context of Brazil's elections. The recommendations stress the close relationship between violations of personal data protection and challenges to the integrity of electoral processes. They underscore how privacy and...

DEEPLINKS BLOG BY MARIO TRUJILLO | AUGUST 26, 2026

A List of ICE Subpoenas to Tech Companies

This is likely an undercount. The full scope is hard to pin down because these subpoenas typically only come to light when a user is given notice and challenges them in court, or when a company documents them in a transparency report.

EFF Statement on Meta Settlement

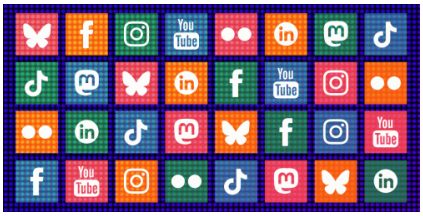
DEEPLINKS BLOG BY DAVID GREENE | AUGUST 26, 2026

The settlement enshrines Meta's harmful surveillance into law, and it will compromise users' privacy and anonymity while increasing their exposure to data breaches and government data requests.

DEEPLINKS BLOG BY VERIDIANA ALIMONTI | AUGUST 20, 2026

Intermediary Liability in Brazil: The Intricate Path Ahead

Brazil's new internet intermediary liability regime is underway. The implementation of changes established by the Supreme Court includes notice and takedown mechanisms and duty of care obligations. Caution is crucial as these measures can create problematic incentives for enforcement overreach and over censorship of protected speech. The...



DEEPLINKS BLOG BY MARIO TRUJILLO | AUGUST 19, 2026

Some Tech Companies Have Privately Pushed Back on ICE Subpoenas. They Should All Do More.

When companies receive these unlawful subpoenas, they should be clear with the public that they will not hand over the data unless a court compels them to do so.