

Evaluating OGO concerns about federal surveillance into Berkeley officials discussing matters of immigration

Question:

Possible changes were introduced to the Open Government Ordinance (OGO) via the OGC (Open Government Commission) that would ban the use of ephemeral, encrypted messaging apps such as Signal by city officials. Concerns were presented regarding a possible situation where city officials want to communicate privately in order to protect undocumented individuals from federal immigration enforcement officials, and they may prefer to use Signal-like technology in these scenarios. This document examines and evaluates such concerns.

Would banning city officials from using ephemeral messaging meaningfully hinder efforts to protect undocumented individuals from federal immigration officials?

My Argument:

We know that ephemeral messaging is used by officials to hide a variety of information regarding public business that the public would like to know about—this law would create a large positive impact by revealing this. When it comes to ICE looking at city data for immigration enforcement, this is chiefly DMV data and other bulk databases, so to protect undocumented individuals those areas should be the focus. It would likely be illegal for ICE to spy on politicians' phones for immigration enforcement, without a (seemingly improbable) public, judicial warrant. And yet, if they did spy secretly, the usage of end-to-end encryption would make it extremely difficult to read texts without getting direct access to one of the devices in the conversation.

End-to-end encryption largely protects city officials already from almost any method that ICE could use to read sensitive texts, with the sole exception of a judge signing a warrant allowing ICE to seize a city official's phone. Using ephemeral messaging on top of that allows officials to skirt public records laws on a wide variety of relevant topics that the public would like to know about, while offering very little additional protection from federal agencies gaining access.

1. There is extensive evidence that city and state officials have used ephemeral messaging to conceal communications around city business.

By the very nature of ephemeral messaging technology, it is hard to know exactly what information has been hidden in the past. However, the press has reported that police matters, communications with private interests and lobbyists, as well as issues with faulty COVID tests have been hidden.

2. There is limited evidence that ICE can look at personal communications for immigration enforcement, especially not in the covert manner we might be concerned about.

The evidence seems to suggest that the vast majority of intelligence retrieved by ICE is from bulk sources such as DMV records and commercial data brokers, rather than communications between city officials.

To me, covert or automatic collection of city officials' text messages is the main potential concern, not as much subpoenas issued by a judge after due process: What if ICE could use covert means like wiretapping or a secret FISA court order to access city communications intended to protect undocumented individuals? I believe (even illegal) wiretapping would be near impossible if end-to-end encrypted messaging is used, which would be allowed. Any requests for data would have to go through the public, due process of an open court and thus require probable cause. To be frank, many sensitive communications designed to protect undocumented individuals would likely no longer be sensitive after the length of time taken by most legal proceedings.

ICE and congressional committees can issue subpoenas that do not carry the force of law, which can be refused by city officials. If these entities go to a court to request a judge to compel the city official, in cases of overbroad requests, several potential legal defenses exist. By the time these judicial processes resolve, the "time window of sensitivity" during which we'd want these conversations to be private would very likely have lapsed anyway. Of course, ICE could simply ask to view messages between officials via CA Public Records Act, but this would also take time, and such records could be redacted to preserve the privacy of individuals involved.

3. Banning ephemeral messaging is very narrow in scope

In general, the intent behind banning ephemeral messaging is in scope a small restriction that may have outsized positive impact by discouraging the attempted avoidance of public records laws by city officials across the entire gamut of city business.

This does not prevent the use of other avenues for privacy preservation such as:

- end-to-end encryption
 - When end-to-end encryption is properly used, one can assume that the only way a third party like a federal agency could access such communications is by gaining direct access to one of the original devices involved in the communication (remote access by installing a virus/spyware, or physical access). NSA etc. could **not** simply ask Signal, a phone provider, internet provider, Apple, etc. for the messages, because those providers don't have the ability themselves to see any messages.
- simply having naturally "ephemeral" conversations in-person or via phone call.
- records retention schedules which would fully allow the deletion of intermediate text messages after some timeframe.
- deleting documents which are already exempt from CA Public Records Act, i.e. for privacy reasons, as long as official is not in violation of 18 U.S. Code § 1519 which deems it illegal to destroy any document even in anticipation that it may be requested by a federal agency for an investigation.

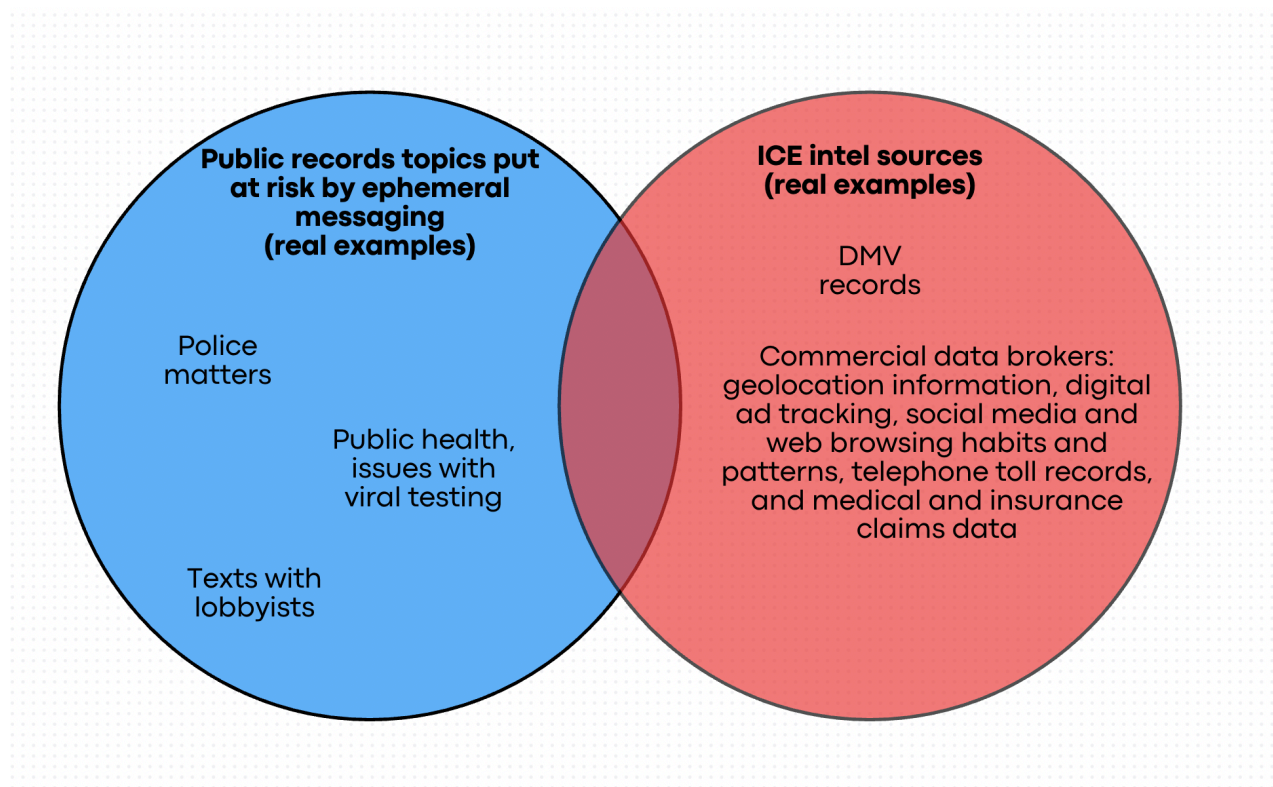


Figure 1: venn diagram. The blue area contains information reported to be hidden from the public via ephemeral messaging, which is of course only a subset of the ideally transparent information which we could help surface. The red area contains ICE intel sources, most of which are unrelated to city official texts. Even if ICE were to gain access to city official texts, I believe an public business ephemeral messaging ban is (a) very narrowly tailored, it still preserves most privacy rights of city officials, and (2) serves a compelling interest of the public. If the aim is to protect data on undocumented individuals from federal access, items in the red circle should be the arena of action. I argue that the intersection itself between these is almost nonexistent, or so much smaller than the benefits in the "blue" that we should pass this law.

Background Information:

What is end-to-end encryption, ephemeral messaging, and Signal?

End-to-end encryption is a technology that, when implemented and used correctly, lets two people exchange messages so that third-parties like the companies and networks carrying those messages cannot read their contents — a protection widely trusted by security experts, though it depends on the users' own devices being secure.

Ephemeral messaging is a technology that automatically deletes messages after they are read or after a set period of time, with the aim of limiting how long communications persist on devices and servers — a useful safeguard against later access, though one that reduces rather than eliminates traces, since recipients can screenshot a message before it disappears.

The Signal Technology Foundation is a nonprofit that built the following:

1. "Signal," an end-to-end encrypted messaging app with ephemeral messaging options. Signal is generally considered to be the most privacy-preserving messaging app, because their software is open-source and they significantly minimize the metadata they store.
2. The "Signal Protocol," an end-to-end encryption algorithm that is used by encrypted messaging providers such as Facebook Messenger, WhatsApp, and the Signal app itself.

Could FISA courts be used to (covertly) access politicians' texts?

I believe the answer is generally **no**, given the right precautions are taken.

The Foreign Intelligence Surveillance Act (FISA, 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871) is intended to conduct surveillance to prevent foreign espionage or terrorism. The courts that authorize spying under this act are famously "closed docket," and fully hidden from the public.

FISA allows warrants against a U.S. person in the following cases:

- If there is probable cause to believe the citizen is knowingly acting as an "agent of a foreign power."
- Section 702 allows the government to vacuum up the communications of foreigners overseas without a warrant. Because those foreigners inevitably communicate with Americans, millions of American emails and texts are "incidentally" swept into the NSA and FBI databases. According to the [Brennan Center](#) and my other research, I believe

that only the FBI, CIA, NSA, and National Counterterrorism Center use FISA and section 702. Section 702 of the Foreign Intelligence Surveillance Act (FISA) is currently expired. It lapsed on June 12, 2026—however, it may still be operationally in effect.

- "Section 702 only permits the targeting of non-United States persons who are reasonably believed to be located outside the United States. United States persons and anyone in the United States may not be targeted under Section 702. Section 702 also prohibits "reverse targeting"—the IC may not target a non-U.S. person located outside the U.S. if the purpose of the collection is to collect information about a United States person or anyone located in the United States." ([intel.gov](https://www.intel.gov))

In other words, (1) ICE does not directly use FISA, though theoretically they could gain access to section 702 intelligence gathered by other intelligence agencies, but (2) the only communications that could be retrieved in our case is if a city official is communicating with a foreign person, not another city official.

Could ICE administrative subpoenas be used to access politicians' texts?

Under the tenth amendment's [anti-commandeering doctrine](#), the federal government cannot compel state or local officers to administer a federal regulatory program. City officials can generally refuse requests from ICE until a judge signs a subpoena.

What about Members of Congress requesting information from cities?

"San Francisco and San Diego, two of California's largest sanctuary cities, are under federal investigation for the alleged actions of local officials who stonewalled ICE and let criminal migrants walk free, The California Post has learned... The committee demanded documents and communications about each agency's interactions with ICE, policies involving non-US citizens, the number of ICE detainers received and declined, and communications with local officials about immigration enforcement." ([Media, House Judiciary Committee](#)).

Again, it seems a city could refuse, and argue in court protection under the tenth amendment.

Then, how do federal immigration officials usually access local data?

The evidence seems to suggest that the vast majority of intelligence retrieved by ICE is from bulk sources such as DMV records and commercial data brokers that provide, for example, location data of cell phones.

According to the Immigration Legal Resource Center ([ILRC](#)), ICE uses administrative warrants to request information from local schools, social services departments, and more. However, the [ACLU](#) outlines: "First, any gag order in these subpoenas has no legal effect; you are free to publicize them and inform the target of the subpoena. Second, you do not have to comply with the subpoena at all, unless ICE goes to court—where you can raise a number of possible objections—and the court orders compliance.

[The CATO Institute](#) outlines a primary source of intelligence for ICE: "the most dangerous and far-reaching tools the government uses to violate Americans' rights over the past several decades come from the private sector, usually in the form of personal data about us, or generated by us, which is then leveraged by commercial data brokers and sold to whoever can pay for it. Such data include geolocation information, digital ad tracking, social media and web browsing habits and patterns, telephone toll records, and medical and insurance claims data. This and so much more is available for purchase by law enforcement at the federal, state, and local levels."

According to [The National Immigration Law Center](#) (NILC), ICE routinely accesses state DMV data indirectly through Nlets (the National Law Enforcement Telecommunications System) or state-specific criminal justice platforms. Because ICE is recognized as a law enforcement agency, they can query these centralized hubs to pull state data that the state itself would not hand over directly. They also cite: "In fact, ICE ERO field offices appear to communicate regularly with state DMVs by email or other informal means that are unregulated and unaccountable. Despite any claim to the contrary, email exchanges appear to occur whether or not an automated system has been used. The communications have included: obtaining driver's license photos, obtaining a range of information about the license-holder or vehicle registration, and offering to help in the apprehension of a person sought by ICE. The information provided by DMV employees includes materials that would not be available through Nlets."

Relevant federal laws that Berkeley officials would have to abide by

8 U.S.C. § 1373 says that a government entity or official "may not prohibit, or in any way restrict" any official from sending to or receiving from federal immigration authorities information regarding the citizenship or immigration status of any individual. This means that a city official cannot prevent another city official from sending such immigration information. However, I'm not sure if this would be directly relevant to messages between city officials.

18 U.S.C. § 1519 deems it illegal to destroy any document even in anticipation that it may be requested by a federal agency for an investigation.