Stop texting like teenagers – Communication in an era of digital government

Have you ever accidentally texted the wrong person? Have you felt the shameful and embarrassing realization almost instantly, resulting in a frantic awkward apology and message deletions?

Technology has made casual missteps omnipresent, with butt-dials and autocorrect disasters. Everyday users are constantly learning and grappling with new phones and software updates, resulting in silly and frivolous online accidents. But when an online group chat discusses classified military operations and includes the Vice President, the National Security Advisor, and the Secretary of Defense, the consequences aren't just awkward or embarrassing. They're dangerous.

Last month, *The Atlantic's* editor-in-chief, Jeffrey Goldberg, was mistakenly added to a Signal group chat where some of the most powerful figures in the federal government were casually discussing and planning upcoming airstrikes in Yemen. The chat, nicknamed "Houthi PC Small Group", was supposed to be a communication channel for a few people, National Security Advisor Mike Waltz, Vice President JD Vance, and Secretary of Defense Pete Hegseth.

They used slang and shorthand text lingo, sending messages with emojis like "👊US🔥," in response to locating an enemy target in a collapsed building. This incident showcased how digital habits that feel normal in everyday life are now leaking into the most sensitive spaces of government, and how that casualness is threatening national security in the process.

The Goldberg incident wasn't just a rogue moment of poor judgment. It was the inevitable result of letting technological convenience overrule professionalism and security.

The officials involved were talking about classified details of U.S. military operations against the Houthi rebels in Yemen. These types of discussions typically happen inside Sensitive Compartmented Information Facilities, or SCIFs, heavily guarded, electronically shielded rooms specifically designed to keep secrets safe. Instead, the officials were sending them on Signal, a commercial app that deletes messages after seven days by default.

Signal is useful for private citizens who want to avoid data tracking, but not when federal record laws require preserving government communications, especially when they involve military strikes. To make matters worse, the White House had formally authorized the use of Signal for sharing of non-classified information earlier this year as a method of communication that was faster than encrypted government servers but theoretically safer than traditional texting.

What they forgot is that national security protocols exist for a reason of safety, not to make life easier for impatient officials.

For most of modern history, sharing classified information has purposefully been inconvenient. Top-secret conversations happen inside SCIFs rooms free of phones or recording devices. Messages were, and often still are, hand-delivered between agencies in locked briefcases. Even electronic communications must pass through heavily encrypted, government-only systems.

When President Obama insisted on keeping a smartphone in 2009, the NSA had to modify it heavily so that it could only call a handful of numbers and couldn't text, take photos, or browse the internet. Obama understood that protecting sensitive information required giving up convenience.

This wasn't a new idea either. During World War II, Franklin D. Roosevelt and Winston Churchill communicated using a special phone system, engineered to prevent the Nazis from eavesdropping. Even then, technology wasn't trusted, and it was treated with the skepticism it deserved regarding national security.

The Signal leak is not an isolated incident of online carelessness with government information, either. In 2016, Hillary Clinton faced widespread criticism for using a private email server during her time as Secretary of State. In 2023, a 21-year-old Air National Guardsman leaked classified Pentagon documents on Discord.

In some ways, it's not surprising that even high-ranking officials have fallen into the same habits as everyone else. Over the last decade, the line between formal and informal communication in the workplace has steadily blurred. Slack channels replaced meetings, emails turned into texts, and bosses started responding with thumbs-up emojis. The COVID-19 pandemic furthered this shift, normalizing online and remote government work. It became normal, and even expected, for serious decisions to happen instantly, no matter where officials are.

Cultural expectations around professionalism changed faster than our security infrastructure did. But our national government isn't supposed to move fast regardless of caution for professionalism or safety. Treating classified discussions with the same casualness we use for texting about weekend plans is a dangerous erosion of standards.

Most of us can afford a typo or an accidental text when using technology this way. Officials handling the lives of American soldiers and the stability of foreign governments cannot.

Today, officials have access to more sophisticated security systems than ever before. SCIFs are located in embassies, military bases, and even mobile units that travel with top officials. Secure

phones, email, and video calls are all available to them. Yet somehow, messaging on Signal still became the preferred method of this administration.

Waltz has claimed the addition of Goldberg to the group chat was an innocent mistake caused by an error in saving the wrong number to a contact card. In the world of everyday texting, that reasoning is understandable. In the world of classified national security matters, it’s inexcusable.

The entire purpose of protocols, like with classified meetings and secure servers, is to eliminate the possibility of human error. Sitting face-to-face inside a sealed room, you can't accidentally message the wrong person or have classified discussions deleted after a week when everything is automatically archived under federal records law.

A new pattern has emerged with technology, with casualness, negligence, and the use of personal technology that falls below the highest levels of discipline. These aren’t tech problems. They’re cultural problems.

Technology isn’t the enemy, carelessness and casual use of them for serious matters is. Encryption apps like Signal, when used properly, can enhance privacy and security. But when the people using them to discuss war plan communications as if it’s a fraternity group chat, no platform is safe enough.

The government doesn't need better apps, it needs a cultural shift back toward treating classified information with the seriousness and respect it demands. Officials at the highest levels of government need to act like stewards of national trust. After all, we expect more caution from teenagers about what they post online. Shouldn't we expect at least that much from our leaders?