# Journalist Security in the Digital World: A Survey

## *Are We Using the Right Tools?*

BY JAVIER GARZA RAMOS

March 2016

CIMA
CENTER FOR INTERNATIONAL MEDIA ASSISTANCE

NED
National Endowment for Democracy
*Supporting freedom around the world*

# Journalist Security in the Digital World: A Survey

## Are We Using the Right Tools?

MARCH 2016

## Contents

### ABOUT THE AUTHOR

**Javier Garza Ramos** is a journalist based in northern Mexico. Currently he is developing a program on media development and press freedom in Latin America for the World Association of Newspapers. He was a Knight Fellow at the International Center for Journalist specializing in journalist protection and digital security. Garza is a former editorial director of *El Siglo de Torreón* in Mexico and has worked with several organization on freedom of expression issues.

CIMA
CENTER FOR INTERNATIONAL MEDIA ASSISTANCE

### ABOUT CIMA

The **Center for International Media Assistance (CIMA),** at the National Endowment for Democracy, works to strengthen the support, raise the visibility, and improve the effectiveness of independent media development throughout the world. The center provides information, builds networks, conducts research, and highlights the indispensable role independent media play in the creation and development of sustainable democracies. An important aspect of CIMA's work is to research ways to attract additional U.S. private sector interest in and support for international media development.

CIMA convenes working groups, discussions, and panels on a variety of topics in the field of media development and assistance. The center also issues reports and recommendations based on working group discussions and other investigations. These reports aim to provide policymakers, as well as donors and practitioners, with ideas for bolstering the effectiveness of media assistance.

Center for International Media Assistance
National Endowment for Democracy

1025 F STREET, N.W., 8TH FLOOR
WASHINGTON, DC 20004
PHONE: (202) 378-9700
FAX: (202) 378-9407
EMAIL: CIMA@ned.org
URL: http://cima.ned.org

Mark Nelson
SENIOR DIRECTOR

NED
National Endowment for Democracy
*Supporting freedom around the world*

# Introduction

A journalist in Latin America wishes there was an application that allows him to report his location while on a risky assignment. A journalist in Central Asia wants a tool to evaluate the dangers in certain regions he covers, because he is "scared on assignment." Other reporters in South Asia say they need tools for keeping data online securely, while colleagues in Western Europe want easier tools for encrypting their mobile devices.

What these journalists probably don't know is that their wishes have actually come true: Such tools exist. They're just not aware of them.

The needs for security tools that journalists around the world have are vast and diverse. Journalists have become more vulnerable not only while on assignment in dangerous places, but also in their daily routines, at home, in the newsroom, or on the road, as digital surveillance increases.

The digital world has made journalism a riskier profession. But it can also make it safer. Digital technology can offer tools to minimize the dangers, whether physical, digital, or psychological, that reporters and editors face on the job. The increasing use of mobile devices among journalists has been accompanied by a stream of applications that apply security layers to their work.

*The digital world has made journalism a riskier profession. But it can also make it safer. Digital technology can offer tools to minimize the dangers, whether physical, digital, or psychological, that reporters and editors face on the job.*

But before media support organizations can help make those tools available, they must first find out what journalists know. Are they aware of such tools? Do they use them? Do they know how reliable they are?

For this purpose, the Center for International Media Assistance carried out a survey of journalists around the world, asking them about their use of digital tools for their security. The survey was designed to address both tools for physical protection as well as digital security.

The survey was disseminated with the help of international organizations such as the International Center for Journalists, the Committee to Protect Journalists, the International Women's Media Foundation, IREX, Global Journalist Security, Article19, and the Open Tech Fund.

The results will help us understand better the need that journalists have for digital tools that can enhance their physical or digital security. The responses suggest important areas of opportunity for new applications or programs that can mitigate risk, either in a specific areas of coverage or in daily work routines.

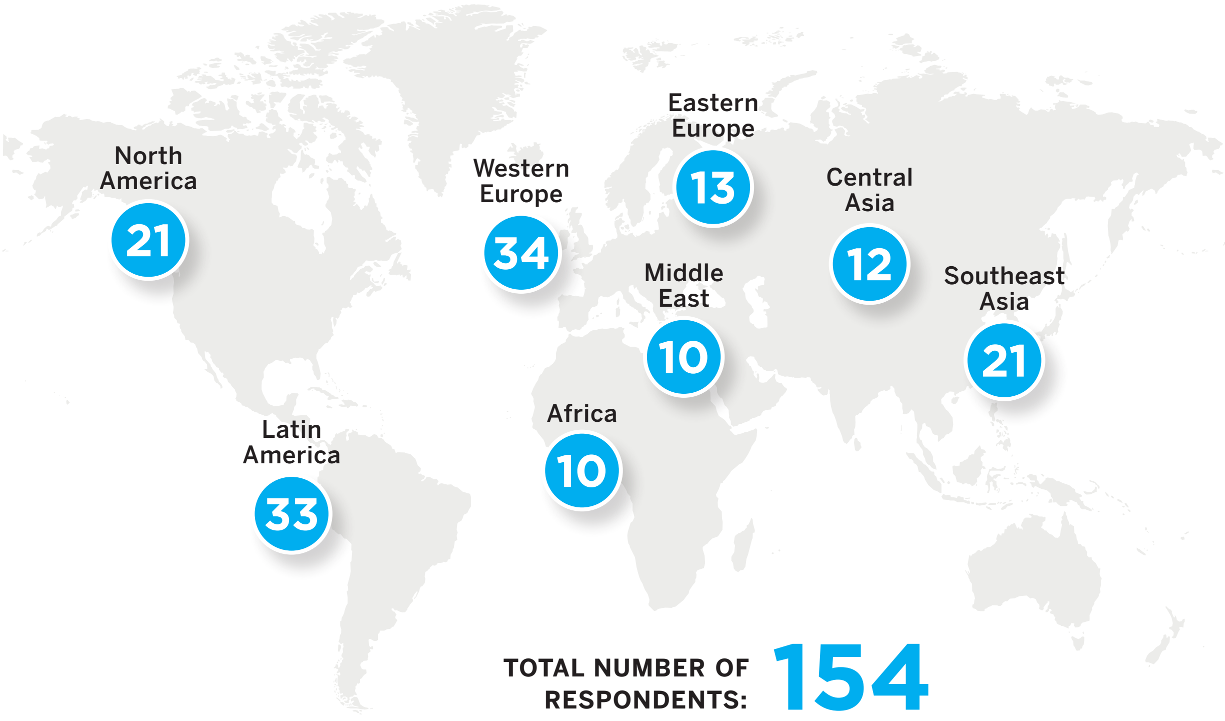
# The Survey

An online survey was conducted during August and the first two weeks of September of 2015. A total of 154 journalists responded from North America, Latin America, Western and Eastern Europe, the Middle East, Central and Southeast Asia, and Africa. While the number of respondents cannot be considered as representative, the fact that they are reporters and editors around the world that are linked to the networks formed by international organizations suggest that they have a higher level of engagement on issues affecting the safety of journalists.

The first question was about general use of digital tools for security, and the results reveal that most journalists do not include this practice in their general safety procedures, either physical or digital. About 60 percent of respondents reported not using these tools in any situation.

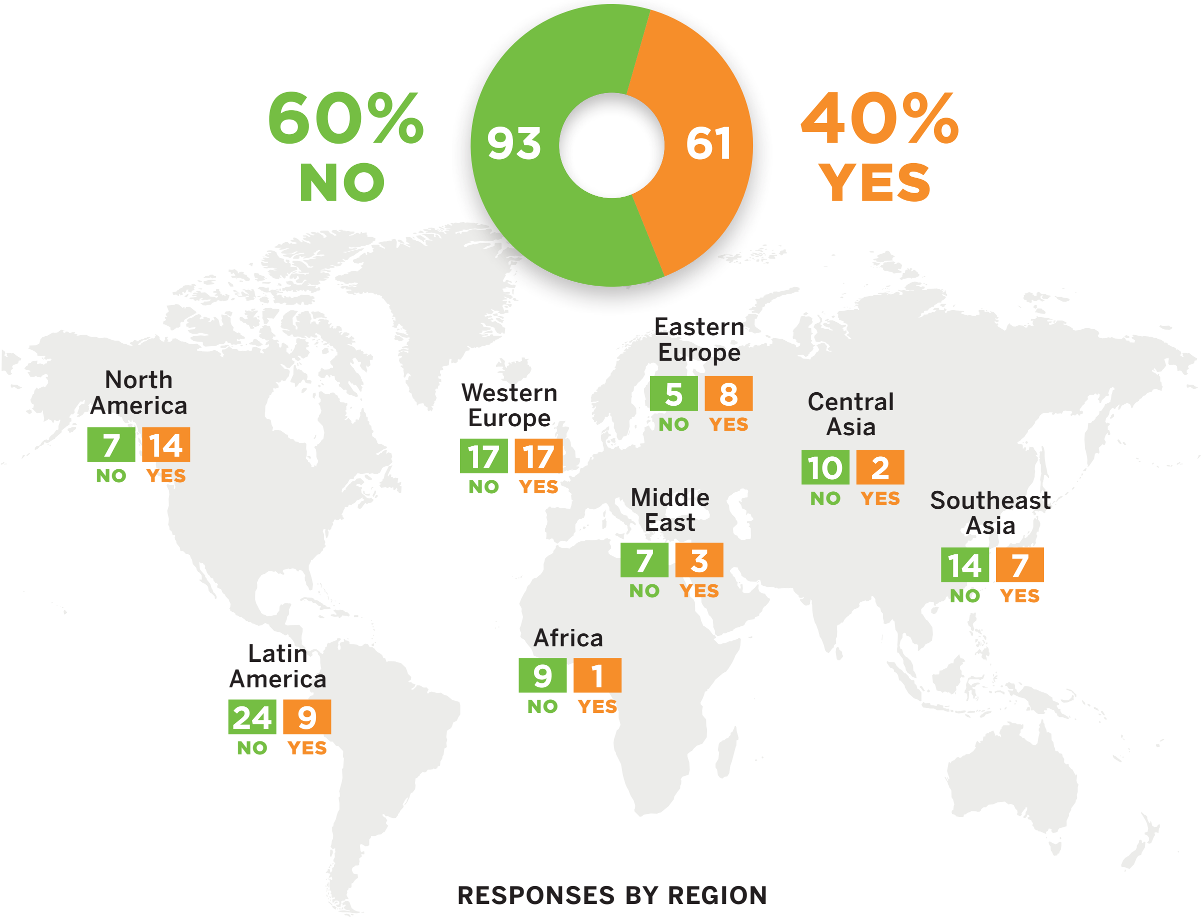
The regional differences in usage reflect the level of assimilation of technology in journalism. As would be expected, journalists in North America and Europe are more likely to use digital tools for security, while journalists in Africa are the least likely.

## Geographic Distribution of Responses to the Survey



## Use of Digital Tools for Journalist Security

Do you regularly use digital tools for general security?



**RESPONSES BY REGION**

However, as we will see in the detailed responses, the survey also reveals that in some cases, journalists think they are using security tools that are not really secure. Asked about tools they use for safely conducting certain activities (communications, sharing documents, etc.) some respondents mentioned tools that are not designed for secure purposes or that have vulnerabilities. In other words, the tools they think that are secure, are actually not. This suggests that while there is an awareness of the need for security, there is little education about what is safe to use.

The survey looked at whether or how journalists use digital tools for different activities: protecting communications, securely storing or sharing files, encrypting their digital devices, allowing trusted networks to track their location during a risky assignments, carrying out risk evaluation and analysis before a dangerous assignment, and consulting online resources such as security manuals, guides and protocols published by specialized organizations. It also inquired about specific experiences in which they have felt the need for a digital tool.

In some cases, the tools the journalists said they need already exist, but in other cases their responses can be taken as opportunities to develop new tools.

# The Responses

## Communications

Protecting online communications (e-mail, chat or voice) had one of the highest rates of positive responses among journalists, although the number of people saying they use at least one tool for this purpose was 30 percent. No journalist from Africa and Central Asia reported using these tools and only a handful from South Asia and the Middle East said they do.

The level of awareness for protecting online communications is higher in North America and Western Europe, which suggest a growing need for tools to avoid surveillance, in the wake of revelations about data-mining and hacking carried out by governments in these regions.

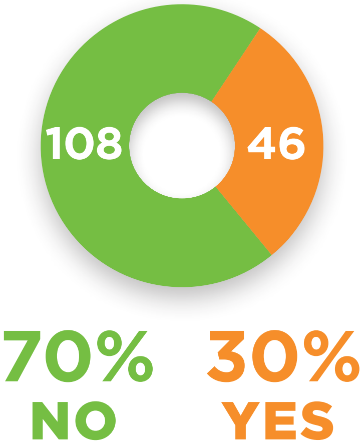
After the emergence of Wikileaks and the revelations about the National Security Agency's surveillance programs by Edward Snowden, many journalists have become concerned about—and skilled in—digital security. There is also a growing awareness among journalists that government, businesses, and criminal organizations around the world engage in online surveillance.

The journalists that protect their communications mentioned tools such as the encrypted web-bases services Riseup and Hushmail, several providers of **PGP encryption** for e-mail, encrypted messaging services like Peerio, Chatsecure and Textsecure, as well as Jitsi, Cryptocat, Adium, which are not for mobile devices. Redphone is used for encrypted Voice over IP. After the completion of the survey Open Whisper Systems, the developer of TextSecure and Redphone, announced that both applications merged into one product called **Signal**, so this app does not appear in the responses even though some users are familiar with its predecessors. Some respondents also said they communicates with colleagues over a **Virtual Private Network** or using the Tor browser for hiding their location.

However, some journalists mentioned using applications that have weak security or are not secure at all. One in Western Europe reported using WhatsApp as a secure form of communication, but when the survey was conducted WhatsApp was barely rolling out its end-to-end encryption and the feature was limited only to phones with Android operating system and did not work on group messages and multimedia. Another journalist, also in Western Europe, mentioned using the app Telegram in encrypted mode, even though there have been doubts about the effectiveness of this feature. This suggests that journalist might not be sufficiently trained to distinguish between safe and not-so-safe applications.

### Secure Communications

Do you use digital tools to protect communications? (Encryption for telephone calls, e-mail, chats.)



## File storage and sharing

Storing and sharing files in a secure manner to guard against unwanted intrusion in a journalist's work is a practice just as common as protecting e-mails, messages, or voice communications, but it is still not widespread. As was the case with digital communications, about 30 percent of respondents said they regularly protect their files when storing them or sharing them with colleagues. The regional breakdown of the responses is also similar, because the same journalists that reported using tools to protect communications also take care to protect files. The correlations between both activities among respondents is almost 100 percent.

The awareness of a need to protect files also springs from the revelation of surveillance programs by governments in the United States and Europe. In fact, the tool most mentioned by respondents is **TrueCrypt**, the same encryption system used by Snowden, but most of the journalists that use it are in Western Europe and North America. While there has been some debate about its effectiveness because its development was discontinued in 2014, it is still favored by many journalists, since some of the flaws that were pointed out were not regarded as a threat to the tool's integrity. A new project called **VeraCrypt** was launched to maintain and update TrueCrypt's code, making it a reliable alternative, although it was not mentioned in the survey.

After **TrueCrypt**, the most mentioned tools were **Spideroak** and **Tresorit**, for storing and sharing on clouds; **OnionShare**, a new application for file-sharing that sends data over the Tor network; and **Virtual Private Networks**.

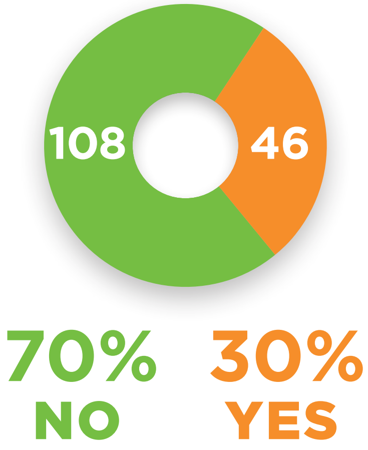
Some respondents said they share files via Web-based encrypted e-mails such as **Hushmail**, but they did not specify if they also use it for storing, while others said they protect documents with **passwords**.

Other respondents said they use Web-based tools such as **SecureReporter**, the website managed by ICFJ to share information between journalists working on collaborative projects. This suggests an opportunity for development of similar tools on a local basis.

It's worth mentioning that some of these tools allow only file storage or only file sharing but not both. In this area there are also journalists that are using unsecure tools that they think are secure. Some respondents said they use Google Drive or Dropbox as "encrypted tools" for storing and sharing files, apparently unaware that neither is actually encrypted nor considered safe.

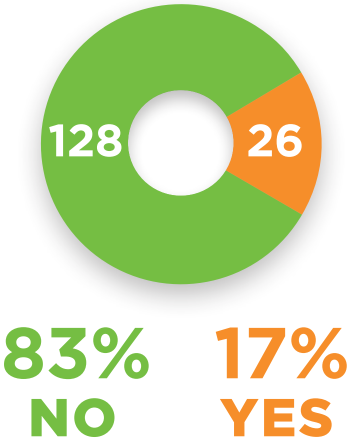
### Secure File Storage/Sharing

Do you use digital tools to share information or documents securely? (Websites or programs that allow journalists to share files during common projects.)



## Device Encryption

Do you use digital tools for device encryption? (Encrypting laptops, tablets and mobile phones to avoid searches.)



## Device encryption

Encrypting devices such as computers, tablets, and smartphones is a less common habit among journalists, with only one in five participants in the survey saying they follow this practice. However, there appears to be an increasing number of converts to device encryption, after reporters have told stories about their digital devices searched or seized by border guards at checkpoints or by police and military forces or criminal groups in high-risk areas. For journalists, encrypting devices, particularly mobile ones, has become a necessity to avoid having important and sensitive data falling into the wrong hands.

Journalists who acknowledged encrypting files for storage probably place more importance on hiding sensitive data from prying eyes. Some of them might prefer to have encrypted files stored in a cloud so they wouldn't have to carry it on a hard drive, leaving important information out of their portable devices.

Others would prefer encrypting hard drives or files so that sensitive information could not be accessed if they lose their devices. In the survey, journalists mentioned using tools such as **WinRAR**, the **built-in encryption features** in their operating systems, **Ubuntu** disk encryption, **BCrypt**, or **Cyanogenmod**, although the last one has been noted for installation problems. Others mentioned protecting documents behind passwords, but this practice has some vulnerabilities because if they are not properly stored, the files can be subject of brute force to break the passwords.

*Reporters have told stories about their digital devices searched or seized by border guards at checkpoints or by police and military forces or criminal groups in high-risk areas. For journalists, encrypting devices, particularly mobile ones, has become a necessity to avoid having important and sensitive data falling into the wrong hands.*

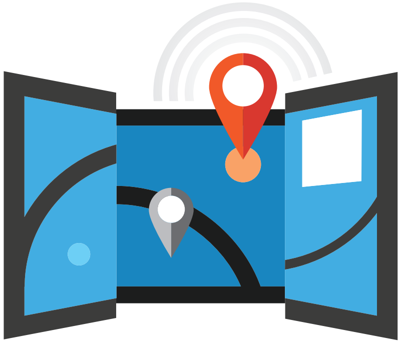
## Geo-tracking

Reporting often entails going into dangerous places, with a higher risk of "falling off the radar," losing communication with editors or colleagues. Reporters can get beaten up and end up in a hospital, get lost in an unknown city, stray into unfamiliar territory, or be kidnapped and held by hostile actors. The risk scenarios abound and can play out anywhere, from the valleys in the Middle East to the slums in Latin America or any North American or European city. Recently, several organizations have begun to develop mobile applications that allow journalists to be tracked via GPS by a trusted network of colleagues or relatives when going on a risky assignment. The apps allow reporters to check in regularly with the network, leaving a record of his movements and locations. If something bad happens to the reporter, the app can send a distress message or alert when the reporter stops checking in.

However, these applications do not seem to be well known. In the survey, only 15 journalists said they regularly use digital tools to establish their locations. Even among this number, not everyone was aware of special apps designed to track a reporter's movement by a network of colleagues. Some respondents said they use mapping sites, such as Google Maps when planning coverage in a certain region, but this is far from establishing a geographic track. In a comment, one European journalist warned that "a lot of people trust the wrong people," casting doubt on whether geo-tracking by a trusted network can be widely adopted by skeptical journalists.

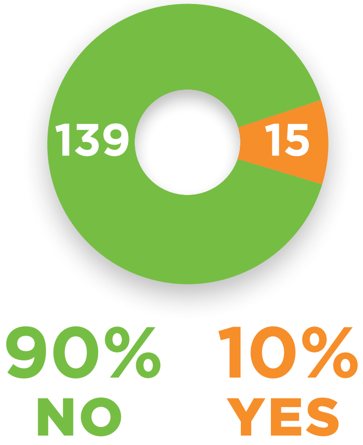
But other journalists said they have tried two tools that have been developed recently by non-governmental organizations: Reporta, launched by the International Women's Media Foundation, and Panic Button, by Amnesty International and Frontline Defenders. Both rely on a journalist's tight circle of colleagues or relatives that can be trusted to respond quickly to an emergency and, in some cases, to keep the location data secret. This suggests another area of opportunity for spreading awareness about the existence of these tools or developing new ones that allow journalists to maintain a lifeline to their workplace or home when doing a risky assignment.

**Reporta** was being tested at the time the survey was conducted and some respondents said they were using it. When the app was announced in September 2015 it was criticized by technology experts because its code was not available for review and it showed weaknesses in its encryption and its handling of personal data. IWMF worked to address these issues but the app remains very useful for journalists at risk in the field. Several journalists working in dangerous environments have used it despite its flaws and report good results.



### Geo-Tracking

Do you use digital tools for geo-tracking? (Mobile apps that enable journalists to report their locations to trusted networks in risk areas.)



## Risk Assessment

Before heading into a dangerous area, reporters should know as much about it as possible. For this purpose, digital tools can be developed to calculate the level of risk in a certain area, based on location and the security situation, particularly any previous attacks against journalists. Such a tool can let a journalists know about the dangers he or she would face when going on assignment in a certain region, such as probable aggressions, as well as the likelihood of receiving medical care or support by local journalists.

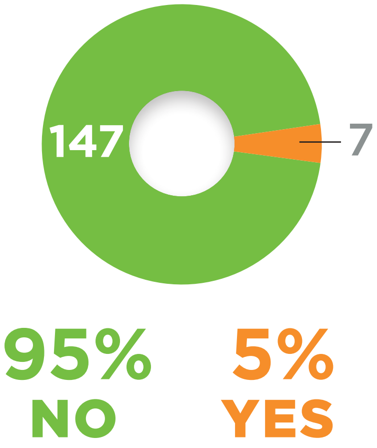
Only seven respondents in the survey said they carry out a risk evaluation before going on a dangerous assignment. These do so by consulting websites about the region they are covering. Two of them also said they rely on mapping services like Google Earth to get to know the terrain.

There are no risk evaluation tools that are widely used by journalists to calculate the dangers of a particular type of coverage, so this is an important area of opportunity. ICFJ is trying to cover some ground with a new app called **Salama**, currently under development. It combines a personal questionnaire of a journalist's security situation with data about attacks against the press in the region to be covered. By taking into account both pieces of information the app can render a measure of risk that can be regularly re-assessed depending on changes in the journalist's or the region's situation.

Another tool being developed is **Umbrella**, an app created by the London-based organization Security First. It offers journalists advice and tips on how to protect against certain physical, psychological or digital threats. The recommendations can be chosen on the basis of ability or type of protection needed, enabling users to get advice suited to their level of risk. There is also a "checklist" to remind journalists what they need to do in each scenario (i.e. how to avoid being kidnapped or what to do in case it happens) and help track progress. Umbrella also includes notifications about attacks on journalists in a user's area. Similar systems can be applied by journalists to measure their level of risk by looking at the history of attacks, the nature of attackers and their methods, as well as an aggressor's capabilities and intentions to arrive at a risk coefficient that would reflect the dangers of a particular type of coverage or region. A similar exercise, asking about security habits and practices, can be used to calculate journalists' digital risk.

## Risk Assessment

Do you use digital tools to do a personal risk assessment? (Apps or websites that allow journalists to conduct individual risk evaluations in their locations or in places you will be covering.)



## Online Resources

Before going on assignment, many journalists set up their basic precautions and security measures based on widely-available protocols designed by specialized organizations. These guides can advise reporters or their editors on what to do in case of emergencies, such as injuries, traumatic shock, threats, digital attack, loss of equipment, arbitrary detention, kidnapping, etc. But the practice of consulting specialized guides before beginning coverage is not as widespread as it should be. In the survey, less than half of respondents (around 44 percent) said they refer to online documents published by news organizations or journalists' associations that provide safety tips, either for physical, psychological, digital or legal protection.

There is a vast array of documents, guides, manuals and protocols on the Web, but the most frequently mentioned in the survey are the ones from the most recognized organizations:

- Committee to Protect Journalists
- ICFJ and IJNet
- Frontline Defenders
- Rory Peck Trust
- Article19
- Free Press Unlimited
- Electronic Frontier Foundation
- Tactical Tech (Security in a Box)
- Fundación para la Libertad de Prensa (Colombia)
- Reporters Without Borders.

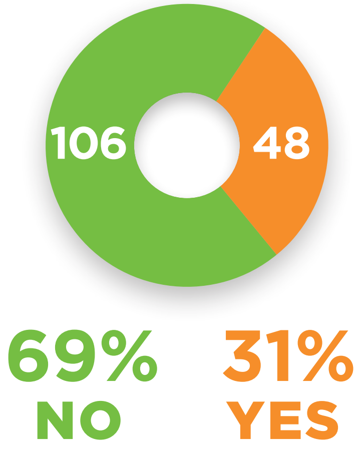
An area of opportunity in this case could be the development of digital tools to pool together the different tips and recommendations given in each manual and each security situation, so there could be a quick way to research advice in a specific type of emergency. This way, a journalist would only need an app to access what all the manuals dispersed on the Web say about a specific security need or situation.

*Guides can advise reporters or their editors on what to do in case of emergencies, such as injuries, traumatic shock, threats, digital attack, loss of equipment, arbitrary detention, kidnapping, etc. But the practice of consulting specialized guides before beginning coverage is not as widespread as it should be.*

© WTO / Flickr (https://creativecommons.org/licenses/by-nc/2.0/)

## Personal Experience

Have you felt the need to have a certain digital tool for safety but did not find one available?



## Personal Experiences

Finally, the survey asked participants if they ever had the need for a certain digital tool but did not find one available. The question attempted to gain a perspective on personal experiences and figure out what the needs of journalists around the world can be in the area of digital tools for security.

Forty-five percent of respondents said they've had a security experience that could have been improved by a digital tool. But when they told of those experiences, it turned out that the tools that about half of them felt they needed already exist.

Some journalists wished they had geo-tracking or risk assessment apps or an easy way to securely store files online, tools that already exist.

Other journalists expressed the need to "prevent hacking of websites," "prevent online hacking beyond strong passwords," or "check devices for security breaches," without realizing that these actions can be done with technology already available. And there are some who just want easier tools, particularly for encrypting devices and documents and detecting if their phones are tapped.

- Other journalists, however, mentioned situations where digital tools can improve their safety, but developing them poses complex technical or logistical challenges. Some tools have already occurred to software developers but cannot be implemented because of technical issues. Others might prove even more difficult, if not impossible. But these needs reflect the concerns of journalists around the world and they can point to ways that can improve their security. For example:

- A journalist in Africa wants an app that tells him "when a Facebook user is arrested in my country." He highlights the vulnerability of journalists, especially bloggers and citizen journalists that are active in political movements and the difficulty of tracking them when a government cracks down on them.

- In South Asia, a journalist mentioned the convenience of having a "comprehensive tool to manage encryption centrally for all devices." This poses technical difficulties because beyond anti-virus software that can wipe out hard drives if they are compromised, there is no way to manage encryption across devices from one place. But the concern suggests an awareness for the need to encrypt devices and the difficulty in managing them.

- A Latin American journalists proposes an “automated risk assessment of the technology I use.” The objective is to measure risk on his devices and share the awareness of digital protections across the newsroom, relying on a network of trusted specialists that would handle the security work.
- One North American journalist wants to have a digital application to “avoid physical surveillance.” While this would involve geo-tracking technology, it is not clear how it would identify active physical surveillance at any given moment, but it reflects a concern for personal security that perhaps could be addressed using technology.
- In Latin America some journalists are asking if there is a messaging service that allows encrypted group chats so trusted networks of local journalists can communicate safely. Most are currently using groups on WhatsApp or Telegram that are not secure. Open Whispers Systems has managed to overcome some technological obstacles and has a group chat function in its TextSecure app, which is encrypted. Cryptocat is an easy tool for encrypted group chats but it is limited to personal computers, not mobile devices.
- North American journalists wondered about the existence of digital tools for measuring stress or applying psychological self-care measures, particularly after a risky or sensitive assignment. While there are no tools specifically designed for journalists, the National Center for Post-Traumatic Stress Disorder (part of the US Department of Veterans Affair) has developed two apps: a **PTSD Coach** that applies a personal check-list of possible PTSD symptoms, and a **Mindfulness Coach** to help practice meditation and reduce stress. Tailoring these tools for journalists might be an area of opportunity in the field of psychological care.

*Forty-five percent of respondents said they’ve had a security experience that could have been improved by a digital tool. But when they told of those experiences, it turned out that the tools that about half of them felt they needed already exist.*

© US Army Africa / Flickr (https://creativecommons.org/licenses/by-nc/2.0/)

## Going Forward

This survey was designed to measure how journalists around the world take advantage of technology to enhance their security. The results suggest that there is a general lack of awareness about the power that digital tools have to improve a journalist's protection. There are scores of organizations of journalists, technologists, and activists developing tools for physical or digital protection or training reporters and editors on how to use them. But there can never be enough education about the risks that journalists face and the security measures they can take, especially when it seems that the press is under attack more frequently and in more aggressive ways than before.

© 1000 Words / Shutterstock.com

*Journalists who have improved their protection with digital tools can educate colleagues about their own experiences, talking about what was helpful or not.*

Against whom do we protect? Governments, criminals, terrorists, security forces? Against what do we protect? Surveillance, hacking, digital censorship, threats? Or worse, kidnappings, beatings? The answers always depend on the place and the circumstances, but technology can help improve any security plan a journalists or a newsroom can design.

The survey also reveals the diversity of the dangers journalists face across regions. North American and European journalists are more concerned with digital protections and more knowledgeable about technology, while those in Latin America, Africa, and Asia give more weight to physical security but are more vulnerable to digital attacks because they don't know about the tools to counter the threat.

Fortunately, the results show that there are many user experiences of digital tools for security around the world, enough to get more journalists involved in using them and in contributing ways in which some of them can be improved. Many tools mentioned in this report are product of organizations looking to improve security in a variety of fields, not just journalism, while others are tailored specifically for journalists. But all of them might benefit from input made by reporters and editors around the world, talking about their security needs or experiences.

Journalists who have improved their protection with digital tools can educate colleagues about their own experiences, talking about what was helpful or not. We can go beyond the toolkits that are available—and that have proven helpful, according to the results of this survey—and

encourage journalists to talk to one another about the particular uses, benefits, or shortcomings of each technology.

Journalist use digital tools every day. They have become indispensable to report, edit, publish, store information, and talk to sources or colleagues. Just as it is impossible to imagine a journalists without a smartphone, and a smartphone without a messaging or social network app, it should be impossible to think about a journalist's digital devices without any security feature.

Around the world, journalists, non-governmental organizations, and technology developers have partnered to imagine and build digital tools for the security of reporters and editors. Enhancing the protection of journalists is an important goal for the media development community, and increasing the awareness and dissemination of these tools would help reduce attacks on press freedom.

*Just as it is impossible to imagine a journalists without a smartphone, and a smartphone without a messaging or social network app, it should be impossible to think about a journalist's digital devices without any security feature.*

© Pavel L Photo and Video / Shutterstock.com

Center for International
Media Assistance

NATIONAL ENDOWMENT FOR DEMOCRACY
1025 F STREET, N.W., 8TH FLOOR
WASHINGTON, DC 20004

PHONE: (202) 378-9700
EMAIL: CIMA@ned.org
URL: http://cima.ned.org

CIMA
CENTER FOR INTERNATIONAL MEDIA ASSISTANCE

NED
National Endowment
for Democracy
*Supporting freedom around the world*