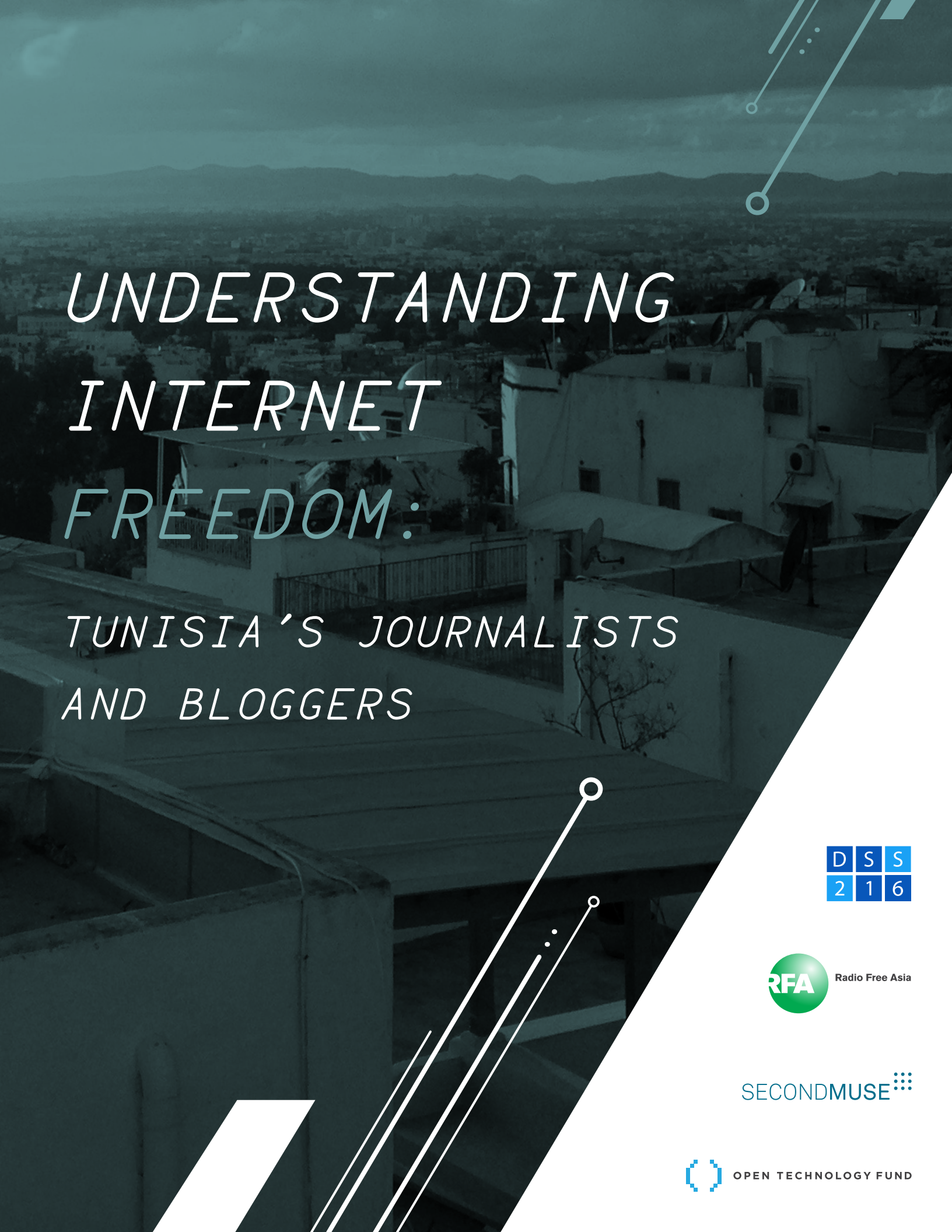


UNDERSTANDING INTERNET FREEDOM:

TUNISIA'S JOURNALISTS AND BLOGGERS

DSS 216

RFA Radio Free Asia

SECONDMUSE

OPEN TECHNOLOGY FUND

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Tunisia has opened up significantly since the revolution that jumpstarted the Arab Spring in late 2010. While media openness and exposure to the outside world has flourished, the legal framework remains a threat to digital rights and freedom of expression; surveillance and harassment of journalists still exists. Positioned at this crossroads, Tunisia demands deeper examination with respect to internet freedom.

In order to deeply understand the needs and challenges that affect journalists in Tunisia, SecondMuse drew on the Internet Freedom Needfinding Framework, which uses human-centered design approaches. Research took the form of interviews with Tunisian journalists, digital security trainers, and intermediary and civil society organizations, followed by a two day Needfinding study with over a dozen journalists, bloggers and webmasters. This report reveals the insights learned about journalists' communication patterns in daily life, security problems and priorities, and communication and safety needs in present-day Tunisia as the country continues to emerge from an era of dictatorship.

The research revealed that many journalists feel they face current and ongoing security risks, both from government and police actors as well as from financially-motivated hackers and companies seeking to use their data. Journalists do employ a variety of security behaviors, although use of specific tools designed to increase digital security was much more limited. Those journalists regularly covering sensitive topics, including politics and protests, were concerned about both digital and physical threats. Those who had already experienced digital attacks often implemented additional security behaviors and were thinking about other ways to keep themselves safe.

Facebook played an essential role in the online experiences of virtually all the journalists we spoke to. It was a source of ideas for stories, the foundation of professional networks, an avenue to publicize their content and, in many ways, an online CV. Facebook's significance as a professional tool also led journalists to develop specific behaviors to protect themselves on that medium.

Through the Needfinding process it became clear that journalists are placing a high priority on getting their jobs done, and done well, and that often serves as a motivation for increased awareness of digital security. Journalists feel deep responsibility for their stories, leading to concerns about how to ensure the safe and complete delivery of their data and footage to their editors. Similarly, they are actively thinking about how to protect the integrity of their data as well any sources with whom they communicate in the course of developing a story. Journalists often face inadequate infrastructure, from limited bandwidth availability to lack of appropriate data storage infrastructure within their organizations, but they develop ad hoc solutions to compensate and deliver their work nonetheless.

The Needfinding process also shed light on a variety of challenges to the adoption of digital security tools and behaviors. Cost of tools was a clear factor, reflected in the common practice among virtually all journalists of obtaining their software free through torrent download sites. Usability also presented a challenge, with overly technical language and user interfaces acting as a deterrent. Those who were interested in making the effort to implement more security measures often felt discouraged by the knowledge that their communications remained insecure due to lack of security on the part of others within their circles.

As Tunisia confronts the conflicting pulls of democratic progress and a repressive history, it is evident that journalists are actively seeking broad sources of information about Tunisia and the world, and are making use of various avenues for self-expression and promotion of their work. While security concerns persist, many journalists are actively exercising their newfound freedoms and are testing its boundaries in many ways.

TUNISIAN CONTEXT

LEGAL CLIMATE[1]

The ouster of president Zine El Abidine Ben Ali on January 14, 2011 was a landmark moment for civil society and freedom of expression in Tunisia. Reaction to that regime led to laws passed in 2014 that protect free speech and ban the prior regime's media censorship. Significantly, Tunisia is now the only country in the world that has in its constitution an article that safeguards access to the internet.[2] There is no internet filtering and authorities have opened up ICT. There is more openness to discuss sensitive issues online such as religion and the army, compared to traditional media. Yet still some online activists avoid crossing the 'red line' over fear of judicial prosecution.

The legal framework remains a threat because Ben Ali laws still exist and there is a new cybercrime agency – Technical Telecommunications Agency (ATT) – which has raised concerns among human rights groups. According to many, the ATT conducts illegal surveillance by monitoring its citizens' online behavior. Without a cybercrime legal framework, people fear a regression in digital rights. In a climate where terrorists are using the internet to recruit and propagate their ideas, it is difficult for lawmakers to understand that some government techniques are harmful to democracy. According to one interviewee, "Terrorism is convenient for people in power, in terms of pushing through legislation that removes rights."

The harassment of citizens persists, with some recent cases of imprisonment on speech-related charges and many reported cases of police "roughing up" journalists. While some infant laws exist it often comes down to the implementation of the law, and the purported police culture of intimidation is endemic. There are decrees that are not implemented widely by judges and police alike. In addition, the judiciary still prosecutes internet users with Ben Ali-era laws such as Article 86 of the Telecommunications Code which finds people guilty when "using public communication networks to insult or disturb others". This leads to journalists having little confidence in the law, and a fear not only for their own safety but for the safety of their sources who are not protected under these decrees.

ONLINE LANDSCAPE

Tunisia is a country where the internet has been in use since 1996 and there has been open access to the internet since the revolution. Ranking 10th in Africa for online usage, 46% of the population is online, and mobile phone use is on the rise. High speed internet costs are high and many Tunisians access the internet at work or from "publinets" (cybercafes), though the latter avenue is decreasing as mobile penetration grows. Both Google and Facebook are extremely popular. 97% of users prefer the Google search engine to other sites, and Facebook penetration is 33% or 3.4 million, with the overwhelming majority under 17 years of age.

Tunisian media is regarded as being open, dynamic and increasingly online. There is an abundance of content on e-newspapers, blogs, and streamed video channels that provide Tunisians a range of viewpoints. As one interviewee put it, "Tunisians are now testing the boundaries of their new freedoms." Digital media is a key part of that. Tunisian civil society uses digital media to get their messages across on social and political issues. Facebook and Twitter are the two most widely used sites to promote content. And, in 2014, an investigative magazine was launched at Inkyfada.com, publishing complex stories in a rich multimedia format.

THE NEEDFINDING PROCESS

The Needfinding process draws on elements of human-centered design, an approach requiring deep understanding of the needs and challenges people face in their everyday environments in order to inform the design of solutions for those challenges. The ability for solutions to achieve their purpose is often hampered by a lack of understanding about the people they are intended to serve. SecondMuse's Internet Freedom Needfinding Framework (internetfreedom.secondmuse.com/needfinding) provides a process for building that understanding of needs through structured engagement with communities around their security-related challenges and behaviors, while respecting their cultural diversity and privacy. The Needfinding Framework is an open process available to any practitioners interested in better understanding user communities to inform solution design, and continues to be developed iteratively, incorporating new knowledge following each application.

DEVELOPING A RESEARCH PLAN

The first step in our research process was to establishing the research goals for the project and identify the specific questions that would serve as a guide for what our team wants to learn and how we want to learn it:

- **What is "meaningful" communication?**
- **What are the priorities for journalists when they are communicating?**
- **How do individuals in Tunisia define privacy and security?**
- **What communication tools do journalists use?**
- **How do journalists keep themselves safe, online and offline?**
- **What are the security-related behaviors that individuals employ in their daily communication activities?**
- **What do users consider when making a security-related decision online?**

BACKGROUND RESEARCH AND INTERVIEWS

In order to prepare effectively for the fieldwork in Tunisia, the research team spent time actively seeking to understand some of the challenges and the realities of the journalists with whom we would be engaging. Extensive background interviews with a wide variety of organizations facilitated that understanding and contributed to the design of the activities, exercises and interview questions utilized during the course of the Needfinding research, and provided valuable context reflected throughout this report. Interview subjects included Tunisian journalists, digital security trainers, members of organizations providing support to journalists or digital security advice and assistance to those under threat, and representatives of well-known investigative journalism organizations operating both during and after the dictatorship.

NEEDFINDING TOOLS AND TECHNIQUES

During the fieldwork in Tunis the research team engaged in multiple activities designed to develop a deeper understanding of local journalists' needs. While understanding insights about underlying motivations is an integral part of this process, simply asking direct questions on security threats and software features is often not the best way to obtain those insights. The Needfinding process draws out those insights and situates them within the broader context of a journalist's work and daily life by employing a range of techniques that include observation, interaction and discussion, allowing journalists to express insights in multiple ways, mediums and environments in order to have a more comprehensive understanding. Some tools used included visual drawing exercises and group drama and storytelling, all of which highlighted communication patterns in daily life, security problems and priorities, and communication and safety needs.

CONVENING THE PARTICIPANTS

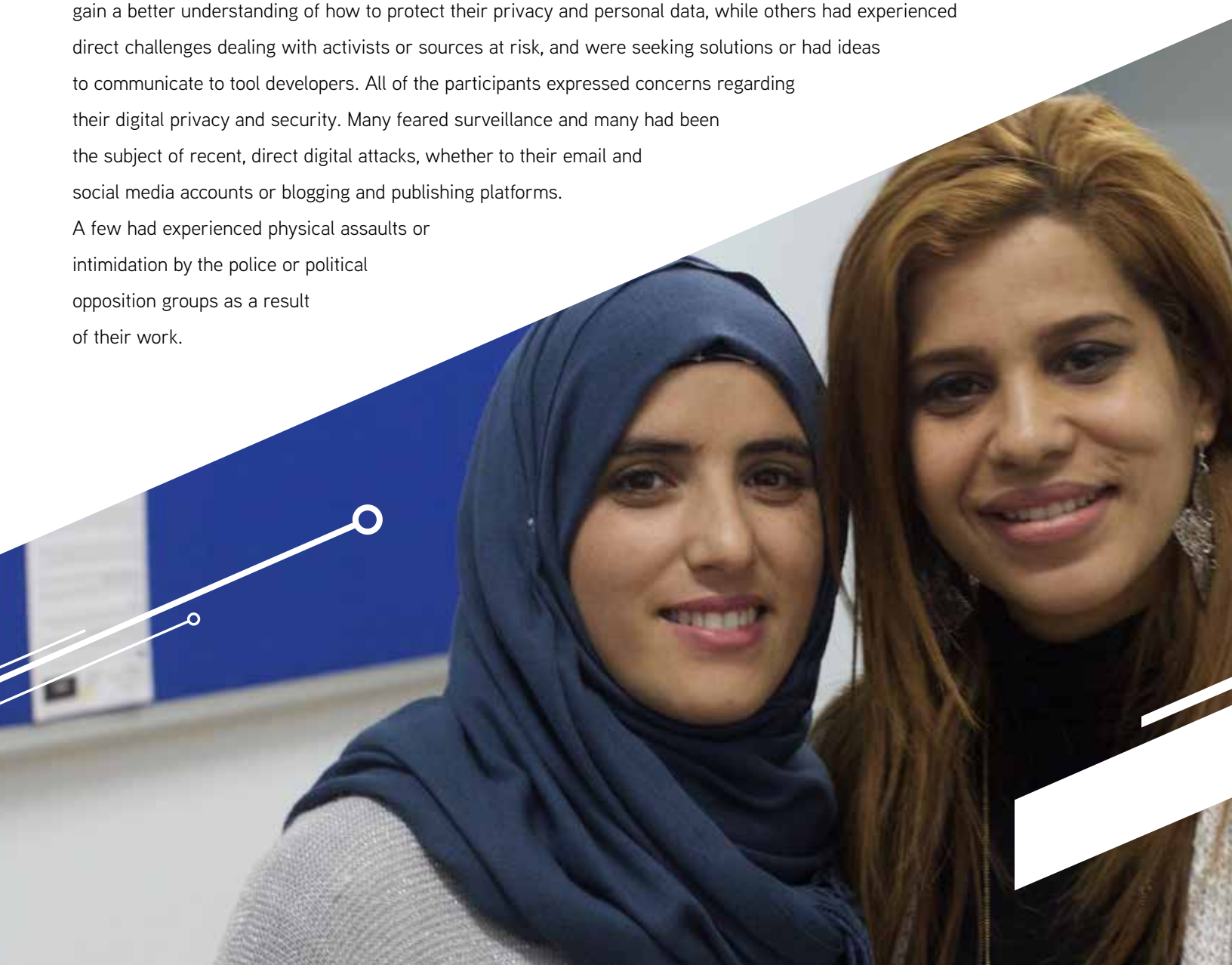
SecondMuse worked with a local Tunisian partner, Digital Security School 216, to convene the group of Tunisian journalists that would participate in two days of Needfinding exercises, aimed at improving the understanding of their day-to-day realities as journalists in Tunisia and their ideas and concerns with respect to privacy and security. In addition to the participating journalists, a French/Arabic translator ensured understanding across languages, and three members of the Digital Security School 216 team joined in the convening, adding valuable local and security-related context to the insights shared by the journalists.

DEMOGRAPHICS

The participating group of eleven journalists was self-selected, each responding to an invitation to take part in a two day Needfinding process regarding digital privacy and security. Notably, the participants were all between the ages of approximately 25 and 35. The participants did not include journalists of older generations, nor was standard print journalism represented within the group. The journalists participating represented a diversity of roles within the field, from television and radio journalists, to proprietors of online newspapers, to webmasters supporting the online presence of news outlets and radio stations, and finally reporters and amateur news bloggers. There were six men and five women, all were university-educated, and though they hailed from a variety of regions within Tunisia, all lived and worked as journalists in Tunis. Within the group, only one person had received past training in digital security.

PARTICIPANTS' MOTIVATIONS

The participants expressed a wide variety of motivations for participating in the Needfinding process. Some hoped to gain a better understanding of how to protect their privacy and personal data, while others had experienced direct challenges dealing with activists or sources at risk, and were seeking solutions or had ideas to communicate to tool developers. All of the participants expressed concerns regarding their digital privacy and security. Many feared surveillance and many had been the subject of recent, direct digital attacks, whether to their email and social media accounts or blogging and publishing platforms. A few had experienced physical assaults or intimidation by the police or political opposition groups as a result of their work.



BUILDING AN UNDERSTANDING

The activities, interviews and discussions that comprised the Needfinding resulted in an outpouring of information relevant the research questions guiding the project, and significant learning about the daily realities of working as a journalist in Tunisia. This learning, detailed more fully below, forms the foundation of the insights and recommendations that ultimately emerge from this Needfinding process.

COMMONLY-USED TOOLS

Knowledge of the digital tools and platforms already in daily use by journalists in Tunisia can assist tool developers by providing insight into the types of digital interactions journalists are accustomed to. All the journalists in the Needfinding made use of both mobile phones and computers in their work, some relying heavily on smartphones to capture photos and video, and even post news stories to blogs and online newspapers. Windows operating systems were used by all the journalists, with the two webmasters for electronic newspapers also utilizing parallel Linux systems for development and testing. Linux was seen as an unrealistic option by many of the journalists because of their reliance on Adobe tools like Photoshop, which are unavailable on Linux. File-sharing programs were identified as important with Dropbox, WeTransfer and Google Drive being the most common. Google Chrome was the most commonly used web browser, and Gmail the primary email client for most of the journalists. Wordpress was cited as the prevalent platform for publication of blogs and online newspapers in Tunisia due to its low cost and customizability. Facebook is the dominant social media platform, with a few journalists also using Twitter and Instagram as avenues to track events or follow cultural issues. Skype was a familiar tool to all the journalists, but used most frequently for speaking to family or interviewing individuals abroad, and less so in the day-to-day context of their work.

THE ROLE OF FACEBOOK

Facebook was a critical professional tool for all the journalists participating in the Needfinding, and is a ubiquitous part of Tunisians' digital engagement; more common that email. "Internet in Tunisia is pretty much Facebook," one interview subject claimed. Many journalists cited Facebook as a source of "preliminary" information from which to gather story ideas and build and understanding of the events and issues the population is interested in. For journalists, Facebook also operates as a form of CV – a mechanism through which they represent their professional selves. For instance, a profile picture is seen as part of a freelance journalist's CV; it enriches the public persona of the journalist which is important to their work. Equally important is their Facebook wall and the nature of information shared or permitted there. Many of the journalists mentioned building their professional networks using Facebook and using it to access contacts to verify stories, as well as receiving tips through Facebook messages from anonymous sources interested in making contact with a journalist.

In Tunisia, Facebook is more than a social platform, it is also political. Facebook was a key tool in coordinating the social action that led to the fall of the Ben Ali regime. It still serves as a platform for organizing and gathering people to "go to the streets," and in many ways it represents Tunisians strong desire for free sharing of information and connection with the outside world. The journalists clearly valued that ability to leverage Facebook as a tool for sharing their own stories. As Facebook is so widely used in Tunisia, there was much commentary throughout the Needfinding engagement about the importance of it in journalists' daily lives. As one journalist said, "Sometimes Facebook can decide your future".

NOTIONS OF PRIVACY AND SECURITY

Communication activities and security-related behaviors are typically rooted in beliefs about privacy. The Arabic translation of privacy, khususiya خصوصية, has multiple meanings and it is a question of where it stops and where it ends. When asked for their ideas about privacy and security, the group agreed that it is mainly about control over one's personal information. Only the individual should have access to their accounts and information and the choice of sharing them should be completely up to the individual. One participant expressed that people can exercise greater freedom if they are convinced that privacy is not important, a sentiment that may provide insight into the behaviors of the population at large.

In terms of what types of information should be held private they cited confidential sources and routine email/message history. For those that worked more with activists, they were concerned about keeping data on their hard disks and smartphones safe and would go to the extent of not communicating details at all via SMS or email, and schedule in-person meetings instead. Ideas of security also extended to the physical realm, as pickpocketing is a daily fear for those in public spaces and journalists on the frontlines are increasingly more vigilant against police or political harassment.

Among the group there was also an underlying mistrust of foreign companies and countries that purportedly collect personal information, combined with the dearth of data protection laws in Tunisia. Add to this threats of state surveillance, and journalists felt skeptical about their data privacy. However many that were most outspoken about this state of affairs simply shrugged it off in resignation, with a 'nothing you can do about it' attitude.

SECURITY CONCEPTS AND TOOLS

While all the participants expressed concern about the security of their information or data, and all were active users of technology tools, the awareness of many well-known digital security tools within the group was limited. Those who were working as webmasters for online news sources had much deeper technical expertise and knowledge of more specific threats, yet still used few security tools.

Password security: All of the journalists were concerned about password security, but had different understandings of what constitutes a secure password and different mechanisms for creating those passwords. Some participants cited using mixed words and numerals, others mentioned changing passwords frequently, and a few created complex passwords and saved them using sites like LastPass and KeePass to avoid forgetting them. One participant built his own algorithm to create complex passwords for himself. Fear of password complexity resulting in forgotten passwords was also an issue. As one participant stated, "I change my password often, and usually use a name or date that is symbolic. Passwords related to personal details are easier to remember."

Two-factor authentication: The journalists using two-factor authentication implemented it after experiencing threats or hacking of their accounts and were searching for ways to better secure themselves. A number of journalists used two-factor authentication for both their Facebook and Gmail accounts. One journalist suffered numerous incidents of hacking in his Facebook account and in attempting to recover them, was instructed by Facebook's support team in how to enable two-factor authentication.

Data encryption: There was a perception that encryption might result in loss of access to data. Many of the journalists had heard of encryption but displayed varying levels of knowledge as to its meaning. None made efforts to encrypt their data, and losing access to existing data was a recurring concern. One journalist said, "If I encrypt my data, it can go the other way around, I won't be able to decrypt it."

Email encryption: Email encryption was of limited utility to the journalists because their contacts do not encrypt their email. None of the journalists participating in the Needfinding used PGP or encrypted email, though most had heard of it. The only two participants to have actually experimented with encrypted mail were webmasters for news outlets, both of whom had more technical training. Both had stopped using it. As one journalist stated, "I don't encrypt because encrypting is not common in Tunisia, and if the counterpart doesn't encrypt it's useless."

Https: Even those journalists who were aware of https still conduct their online activity without regard to whether sites are secure or not. A Tunisian digital security trainer told us "Only experts or IT people know about https, and it is an automatic service, so they deal with https but don't know what they are dealing with." Consistent with that assessment, the only people who were aware of https were those journalists with deeper technical training, like the webmasters or proprietors of online newspapers. Two of the journalists echoed similar sentiments however, stating that while they do pay attention to https, "even official government websites are not secure, so it's the least of our concerns." They also emphasized that their work requires checking content on many sites, preventing them from limiting themselves to https sites.

Tor: None of the journalists had ever used Tor to facilitate their work. While background interviews with investigative journalism organizations and digital security support teams indicated that Tor was often used by journalists and activists under the Ben Ali regime, when asked about Tor most of the journalists participating in the Needfinding were either unfamiliar with it, or had never tried it themselves (barring one who had experimented with it in a digital security training).

Antivirus software: Where journalists used antivirus software, it was typically downloaded illegally through torrents and there was a perception that using antivirus software made your computer slower. Digital security trainers experienced with training journalists in Tunisia shared that analysis of journalists' computers often revealed numerous viruses due to lack of virus protection or outdated/ineffective antivirus software. Among the journalists we spoke to, antivirus software was primarily mentioned in the context of fears that viruses might lead to loss of data, for example video footage. The conflict between speed and security was also highlighted by a few who expressed the sentiment that "the better the antivirus, the slower your computer gets."

Remote disabling: A remote disabling tool or "kill switch" was seen as a way to protect sensitive mobile phone data in the event of theft. With pickpocketing a relatively frequent occurrence, two journalists noted use of a remote disabling tool or "kill switch" as a way of protecting sensitive data on their mobile phones in the event of theft. The tool would allow them to wipe their phone data at the touch of a button, or remotely back-up and then erase the data from the phone after it is stolen, helping to prevent any leaks, for which the journalists would be held responsible.

PERCEIVED THREATS

In discussing the security threats they were facing, it became clear that the journalists felt they were confronting various adversaries. In some cases in describing the threats perceived and attacks experienced, they were uncertain which adversaries were responsible for which threats, knowing they were being targeted but not specifically by whom. Below are the key adversaries mentioned by the journalists:

GOVERNMENT

The primary adversary mentioned was the government, specifically the Ministry of the Interior. Many of the journalists felt confident they were being, or had at times been, under surveillance by the Ministry of the Interior through tapping of mobile phones, and some cited proof of their surveillance based on sources within the Ministry. One journalist believed local ISPs were complicit, saving people's calls, and tracking and reporting movements of cell phone users.

The journalists believe the Tunisian Internet Agency (ATI) acts to censor websites. Journalists cited occasions when they believed ATI would block their newspaper sites and lock them out as administrators for days at a time following publication of sensitive Ministry or other government documents. As one journalist said, "The ATI are the ones controlling all the websites. They can hack into my account. The ATI reports everything back to the Ministry of the Interior and I don't feel like I'm safe."

Police can pose a physical threat to journalists, as well as a threat to their data. Journalists were consistent in identifying the police as their primary adversary in terms of threats to physical safety, as well as threats to their data in the form of confiscation of photographs and camera footage. In one group exercise, the participants prepared a dramatic presentation highlighting the common dynamics of police assault of journalists, calling it one of the "major issues in Tunisia," and focusing on the challenge of recuperating data lost under such circumstances. Three of the journalists participating in the Needfinding had experienced clashes with the police where they had been physically assaulted while covering protests, or where cameras had been confiscated and footage erased. As one stated, "the harassment happens behind the camera."

POLITICAL OPPONENTS

Opposition parties or political opponents also mount digital attacks against journalists and news sites. Some members of the group indicated that reporting or publishing information detrimental to an opposition political party or person had resulted in direct digital security threats, in the form of attacks to the news website, malicious reports of offensive content on Facebook pages resulting in account blocking, and other forms of hacking or interference; or personal attacks toward the reporter in the form of personal accounts being hacked or physical assaults or intimidation.

HACKERS

Journalists used the term "hackers" to refer to anyone engaging in digital attacks, regardless of the adversary. Hackers were referred to both as an adversary in their own right, as well as individuals-for-hire used by other adversaries to execute digital attacks. One journalist of a well-read online news magazine also detailed how hackers had on various occasions hacked into his high-profile Facebook pages and taken them over to sell to advertisers for financial gain. In other cases journalists spoke of the government or political opponents hiring hackers to hack their news websites or hack into their accounts.

DATA MINING

Concerns about data mining for financial or political gain are growing. A few journalists cited growing concern about companies having access to their personal data and potentially misusing it for financial or political gain. In a recent high-profile case in Tunisia, individuals' names gathered from grocery store purchases were used without their permission to file political petitions, highlighting the potential misuse of personal data and drawing attention to that potential threat.

SECURITY BEHAVIORS

Understanding the security behaviors the journalists have developed to respond to the threats they perceive from their adversaries provides insight into their threat models, highlighting the tools and actions they feel impact their safety and casting light on what elements of security they prioritize. Following are some of the security behaviors the journalists have developed to feel safer in their day-to-day lives:

- **Use of coded language or limiting detail in conversations where security risks are heightened:** Some journalists developed code words over time within their trusted networks and employed them in mobile phone conversations in order to discuss sensitive information, like the sharing of a leaked document, or to set up a meeting. One digital security trainer also noted, "In the past we know for a fact they used to surveil based on certain trigger words, like 'Ben Ali'. Here we also think certain words will flag you for surveillance." Similarly, journalists shared the practice of reducing conversations to the fewest possible details, so potential surveillors might know of upcoming events but not the dates or locations.

- **Backing up documents to protect the data and themselves:** Preventing data loss was one primary motivation for backing up information, and particularly sensitive documents. One group of journalists also highlighted the practice of making physical copies of sensitive documents and keeping them in many different places. In presenting their security strategy for a blogger releasing sensitive information, that group emphasized "contacting other acquaintances to [let them] know that if anything happens to the blogger, they will be publishing [the information] all over the internet and making a big scandal."

- **Visibly identifying themselves as press when in public to guard against physical threats and confiscation of data:** Journalists noted that when they could visibly identify themselves as press, they were less likely to be subject to police harassment or confiscation of equipment when covering events like protests because there are laws in place to protect journalists. When not wearing a press vest or other identifier, however, police are more likely to assault them and take their cameras, and then later claim they did not know they were journalists.

- **Arranging face-to-face meetings for sensitive discussions:** Many of the journalists felt face-to-face meetings were safer for exchanging sensitive information than mobile phone conversations or using email and Facebook. Meetings would be arranged through a few brief words on the phone, and then detailed information and documents could be exchanged in person.

- **Using fake or misleading file names for confidential files:** One journalist detailed his practice of naming sensitive files with misleading file names in order to prevent their detection by someone accessing his computer.

- **Limiting the data obtainable from their smartphones:** A few participants suggested that limiting smartphone use made them feel safer. Some barely used a smartphone at all, while others used them only as a secondary device for consuming content rather than for storing any information or making calls.

- **Preemptively increasing server bandwidth in anticipation of attacks:** Webmasters for online news sources noted they paid for increased server bandwidth as a guard against server attacks bringing down their websites.

SECURITY BEHAVIORS ON FACEBOOK

- **Use of private Facebook groups to securely share information and contacts:** The journalists all participated in private Facebook groups, and some noted that such groups were often used to share contacts among themselves and find others to verify tips and information from sources.

- **Creation of anonymous Facebook profiles to post controversial information:** One journalist indicated that he kept himself safe on Facebook by creating anonymous profile pages from which to post potentially controversial blog posts, using profile names like "Tunisian Leaker" or "Minister's Son."

- **Erasing messages in Facebook chat to remove a record of the conversation:** A majority of the journalists participating in the Needfinding indicated having erased Facebook chat messages. As one journalist said, "I am afraid of posting the messages online. I always erase the Facebook discussions." Levels of awareness as to the limited effectiveness of that practice varied.

KEY INSIGHTS AND RECOMMENDATIONS

1 **A newly found sense of freedom in the country has led Tunisians to begin "testing the boundaries of their new freedoms."** The deep integration of Facebook in the lives of journalists and citizens – both as a professional forum for broad self-expression and as a source of information about Tunisia and the outside world – is one avenue through which new freedoms are being exercised. Despite clear awareness of the potential security risks associated with Facebook and other digital tools based on high profile arrests or known instances of surveillance, journalists who did not regularly deal with sensitive material in their work were not actively thinking about security measures. As one interview put it, "Security in Tunisia is less important than freedom. First we need to be free, and then we'll see if we are secure or not."

2 **Products and tools coming from the West face selective skepticism and scrutiny.** Although most of the widely-used digital tools originate from Europe and the United States, there remains a greater suspicion towards products and tools from the West, or funded by the U.S. government, as well as towards foreign companies storing private personal data. Notwithstanding, all participants relied almost exclusively on Western-built tools in their work and there was limited mention of any tools developed in the MENA region.

3 **Journalists prioritized commitment to their stories, frequently expressing greater concerns about the possibility of data loss than about security threats.** Journalists feel a high level of responsibility to complete their work and deliver it in a timely way, often causing them to reject more cumbersome – but more secure – tools. For example, some journalists shared that the pressure to send footage from the field to editors on schedule frequently means using insecure networks to transfer and store files.

4 **Journalists will implement security measures in order to protect sensitive data and sources.** Protecting data and sources was a primary concern of journalists who dealt with sensitive information. They felt strong responsibility to ensure the safety of their sources. As one said, "the law might protect me, but sources are not protected." Similarly, journalists took precautions to avoid potential leaks of sensitive data, aware that they would be held responsible.

5 **Journalists want the freedom on Facebook to broadly share the stories they develop, but they also need to control the content associated with their profiles.** Facebook is a critical tool for the journalists, but given its role within civil society and following arrests for content posted on Facebook, there is also awareness of the platform as a threat. Journalists are weighing their need to widely share information and establish themselves as professionals on Facebook against trying to limit their potential exposure to risk on Facebook through actions like deleting messages and posts, and limiting themselves to private groups.

6 **Journalists seek tools that function effectively with limited infrastructure, often developing ad-hoc solutions in their absence.** Tunisia has narrow internet bandwidth and limited connectivity, particularly in outlying regions, so new tools need to allow for those limitations if they are to be of value for journalists. Many journalists emphasized the challenges of submitting articles, doing research, and safely sending multimedia footage over slow networks, detailing practices like hand-delivering footage by USB in order to ensure safe and complete transfer. In addition, journalists mentioned routinely using Facebook and email accounts to transfer as well as store their material, in response to lack of internal infrastructure within news organizations for storing documents.

7 **People are willing to suffer the inconvenience of using digital security tools once they have been subject to attacks.** Journalists who implemented digital security tools in their lives generally took those steps only after experiencing direct threats to themselves or their work. Tools become a bigger issue, and security a bigger concern, when risks become obstacles to completing their work and they need to seek more secure methods. A security specialist experienced in providing support to Tunisians facing digital security threats noted, "People will only use it if they suspect something. When offering two-factor authentication the platform doesn't say 'hey guys, you may be compromised if you don't do this.' It says, 'please give us your phone number.' If I'm interested in privacy, I'm going to say, 'No, I don't want to give you my number.' People don't try to be more secure natively, they do it when they fear they are under risk."

8 **Cost of tools often trumps security risks.** Cost is a key factor in making choices about digital tools, regardless of the impact on privacy and security. Downloading of virtually all their software from free torrent websites and using pirated versions was a universal phenomenon among the journalists we spoke to. Wordpress is the dominant platform for online news – in spite of security concerns expressed by the journalists and proprietors – simply because it was the cheapest system on the market.

9 **Journalists are deterred from adopting secure behaviors when others in the chain of communication are not being secure.** Journalists were aware that they were only as secure as the weakest link in their communication chain (or social media circle), creating a sense of futility regarding the implementation of more secure practices.

10 **Simple design with default secure settings leads to better user security.** People need simple solutions with security embedded by design, so that users are not required to change or reconfigure tools in order to make them more secure. This counteracts the perception among many journalists that the ability to use secure tools is directly proportional to the technical expertise of the user.

11 **Usability trumps localization.** In Tunisia users are comfortable with digital tools in English, French and Arabic. When asked, journalists rarely cited language or localization as an obstacle to use of digital tools, emphasizing that a user interface that is not too technical in its language, but rather designed with the common user in mind, is a more important factor in determining use.

12 **Tools that are linked to Facebook will have a higher chance of being adopted in Tunisia.** Given Facebook's ubiquity, journalists and citizens are perpetually connected to the tool, giving an advantage to applications that integrate with Facebook seamlessly.

13 **Tools need to take into account physical threats as well as digital threats.** Personal physical safety and the physical protection of their devices and data was of equally high concern to the journalists as their digital security.

14 **Tools should have dual applicability on mobile phones as well as computers.** Many of the journalists continuously transition between their mobile phones and computers as they work, storing and accessing information on both.

PERSONAS

The following personas were developed to help readers better understand the diversity of roles, experiences and challenges reflected within the group of Needfinding participants. In designing solutions for this group, Personas can help those designing solutions for this group think more concretely about what their end users are like.

NOUR: THE BLOGGER

OCCUPATION

Nour is a blogger who writes and takes photographs for an independent e-newspaper, as well as for her personal blog and various other blogs that she contributes to. Nour uses Wordpress and promotes her blogs on Facebook.

BACKGROUND

Nour is 22. She was a teenager when the Ben Ali dictatorship was overthrown, and she became interested and active in politics and civil society work. She studied English at university. One of her university classmates invited her to write blog posts and she became interested in writing and current events.

MOTIVATIONS

Nour is inspired by the revolution and wants to keep issues of freedom alive among her contemporaries and amplify the voice of her generation. Nour is eager to understand new perspectives and views from outside Tunisia and see how they can be applied in her country to foster its growth and development towards a free society.

CHALLENGES

- **Building a trusted network:** Developing a reliable network for stories, fact checking and exchanging information and documents with sources and colleagues is a challenge.
- **Low salaries:** Bloggers make very little money and are often forced to take on multiple assignments.
- **Connectivity:** There is slow bandwidth and inconsistent coverage in Tunisia and Nour is concerned about open Wi-Fi networks since she uses computers at her university and in cafes.
- **Efficient promotion:** Nour wants to be able to share her blog posts across many Facebook groups, but that takes more time than she has.
- **Protection of her accounts:** Nour's Facebook page has been hacked and she has been locked out, requiring assistance from Facebook to recover it. She is concerned about protecting her online accounts.
- **Limited technical knowledge:** Like many of her peers, Nour only has basic knowledge about keeping passwords safe and 2 step verification.
- **Data loss:** Nour's main priorities are protecting her story and meeting her deadline. She is concerned that in transferring data over insecure networks or USB she will lose data, which would also result in not getting paid for her work.
- **Security tools slow her down:** Antivirus software slowing down her system discourages her from consistently using an antivirus tool.

COMMUNICATION

- **Who:** Sources (including confidential sources), government contacts, and other contacts interviewed for stories; editor and web manager of her e-newspaper; other journalists and activists; social network; civil society; her broader blog audience.
- **What:** Local events, arts and culture, and youth movements.

- **How:** Calls and SMS on her smartphone, Gmail, Facebook and Twitter, and applications like Skype and Viber. She uses Wordpress for blogging.

THREAT PERCEPTION

Nour believes her online activity is under surveillance because her Facebook account has been hacked and she hears a tapping or echo on the phone when she is talking. Nour has had various viruses on her laptop. She believes the threat is coming from police or government who are unhappy with things she has written about.

SECURITY PRECAUTIONS

- Nour deletes her Facebook message history because she is afraid of her account being hacked and sensitive information getting out.
- She arranges face-to-face meetings for sensitive discussions and limits the detail she uses to describe where she is going or what she is doing when she uses SMS.
- She changes her passwords every few months and now uses 2-factor authentication on Facebook.
- She has occasionally backed up sensitive documents on a flash drive.
- On occasions where she has a confidential source, she does not write down the name anywhere.

KARIM: THE E-NEWSPAPER EDITOR

OCCUPATION

Karim manages a well-read online newspaper that employs independent bloggers. He writes blogs for the newspaper himself and manages the web platform.

BACKGROUND

Karim is 31 years old. He studied ICT at university and began his employment as a webmaster at a traditional newspaper agency. After a few years he decided to start his own online newspaper. He now hires 3 freelance journalists based in Tunis.

MOTIVATIONS

Karim decided that he wanted to be able to publish his own stories and content more relevant to his generation – including more long-form journalism and investigative work – so he began his own online newspaper, which has grown over the past two years to have a reasonably wide readership among young Tunisians.

CHALLENGES

- **Limitations of Wordpress:** The Wordpress platform is difficult to secure because templates are common, there is no code generator, and it is easily hacked.
- **Server bandwidth:** The server will crash if there are too many people online at the same time so Karim resorts to paying for increased bandwidth to prevent server attacks.
- **Efficient promotion:** Promoting content of his e-newspaper on social media takes far more hours than his team has, and Facebook does not allow automatic cross-posting.
- **Visibility:** Because of his well-known e-newspaper people know his face and he has been vulnerable to attacks from opposition and police as a result.
- **Jack of all trades:** His newspaper relies on him for everything because he is the only person with technical knowledge.
- **Security training:** Karim tries to protect himself online, but others are not taking the same precautions, causing him to believe that some of his efforts are in vain.

COMMUNICATION

- **Who:** Newspaper audience, reporters and sources, government and other official contacts, and telecom companies for hosting.
- **What:** Protests and demonstrations, police crackdowns, politics and government, technology, economics and foreign relations.
- **How:** Wordpress for his e-newspaper; a smartphone for consuming news and information and capturing camera/video footage; and a feature phone for making calls and sending SMS. He uses Windows and a parallel Linux OS and has his own firewall for his site.

SECURITY PRECAUTIONS

- Karim has installed a kill switch on his phone that will let him wipe the contents with a touch of a button (or remotely) if his phone is stolen.
- He set up a firewall for his website.
- He has attempted to use encrypted email, but gave up when no other members of his network use encryption.
- He uses Linux because he feels it is more secure, despite not being able to run common publishing programs such as Photoshop.
- He changes his passwords frequently and uses 2-factor authentication for Facebook and Gmail.
- He uses code words with his close confidantes to share information and set up meetings.

THREAT PERCEPTION

In the past Karim has been intimidated by police and had his smartphone and camera confiscated while reporting on a protest, with the contents wiped. Karim has experienced attacks on his website and on a few occasions his site has been blocked for 3–4 days when he posted information such as leaked government documents. Karim is also concerned about his phone being stolen by pickpockets who would get access to sensitive information. He has various Facebook pages associated with his e-newspaper that have high numbers of "likes," and he is concerned hackers will take over those pages and try to sell them to advertisers. Karim has also had groups organize to bombard him with complaints of inappropriate content in order to get articles taken down.

CONCLUSION

Although only a small focus group of journalists and bloggers were engaged in this Needfinding, key insights and themes have emerged from the process than can assist tool developers in better serving that larger community. Understanding that elements like cost, infrastructure compatibility and usability are high priorities for journalists, and recognizing that protecting data and sources and enabling broad sharing of their work are some of their key motivators, all form part of a larger cycle of design. Uncovering journalists' shared challenges and needs and contextualizing them here is just a first step. With journalists' reliance on tools, technologies and human activities that put them at risk (both real and perceived), solutions will require input and action from several sectors. What needs to follow is a comprehensive, focused cycle of user-informed design that leads to the creation and implementation of solutions responding to those needs. The information and insights collected in this report are as a starting point for developers, trainers, intermediary organizations, policy analysts and funders as they engage in that larger process.

[1]Sources: Individual interviews. Freedom House 2015, State of Freedom on the Net, Tunisia http://www.wamda.com/2013/04/12-key-statistics-on-how-tunisians-use-social-media-infographic; http://nawaat.org/portail/2014/11/14/att-lan-un-dune-surveillance-illegale/

[2]This Constitution, which in Article 31 protects freedom of expression, information and publication, also states in Article 32 that "the right of access to information is guaranteed." Article 24 also includes the protection of private data within constitutional law. http://nawaat.org/portail/2014/11/14/att-lan-un-dune-surveillance-illegale/

This report was written by SecondMuse with support from the Digital Security School 216.

This work was made possible by the Open Technology Fund and Radio Free Asia.

Special thanks to the Needfinding participants, as well as to Access Now, Inkyfada, Reporters Without Borders, the Institute for War and Peace Reporting, Le Forum Tunisien pour les Droits Economiques et Sociaux, and many other independent journalists and security experts who gave us their time and contributed to this report through insights and interviews.

Report layout and design by The Phuse.

SECONDMUSE / secondmuse.com

DIGITAL SECURITY SCHOOL 216 / dss216.net

OPEN TECHNOLOGY FUND / opentechfund.org

RADIO FREE ASIA / rfa.org

Published December 2015