“We have to act like our devices are already infected”: Investigative journalists and Internet surveillance

Philip Di Salvo, PhD

Visiting Fellow, Department of Media and Communications, The London School of Economics and Political Science (LSE)

Post-doctoral researcher, Institute of Media and Journalism (IMeG), Universit àdella Svizzera italiana (USI)
philip.di.salvo@usi.ch

Abstract

Internet surveillance has become a crucial issue for journalism. The “Snowden moment ”has shed light on the risks that journalists and their sources face while communicating online and has shown how journalists themselves can be targets of surveillance operations or other forms of malicious digital attacks from different actors. More recent revelations, such as those coming from the “Pegasus Project”, have underlined even more dangerous threats posed to the safety of journalists, increasingly targeted with spyware technology. Due to the sensitivity of their work and sources and given their strong “watchdog ”role in democracies, investigative reporters are in a particularly dangerous position when it comes to the potential chilling effects of surveillance on the work of journalists. This paper analyzes investigative journalists ’views and self-reflections on the impacts of Internet surveillance on their work by means of in-depth qualitative interviews with reporters affiliated with the International Consortium of Investigative Journalists (ICIJ) and working in Italy, Germany, Hungary, Spain, Switzerland, and the UK. The paper touches on different angles of the Internet surveillance issue by analyzing journalists ’concerns about national and international surveillance players and the overall impact of surveillance on news work.

Keywords

Investigative journalism, surveillance, source protection, information security, whistleblowing

Introduction

The practice of journalism in a digital context brings news challenges and threats, especially in regard to journalists' safety and in particular, to the various possible impacts of Internet surveillance on journalists 'work. According to Lyon (2001), societies that rely on information technologies are de facto surveilled societies, and journalists, as crucial actors of those societies, have to confront this reality. Lyon also states that the Snowden revelations have brought knowledge in "greater detail "about how contemporary surveillance works and with an unprecedented level of evidence (2015, p. 12). The awareness curve generated by the turning point of the Snowden revelations (Coleman, 2019) has also made journalists aware of how being the target of Internet surveillance by hostile groups or institutions (both the state and private entities) is one of the most pressing issues in contemporary journalism (Wahl-Jorgensen et al., 2016). This has become even more urgent in light of recent revelations about the threat posed by spyware technologies to journalists, as emerged through to the "Pegasus Project "investigation in 2021 (Forbidden Stories, 2021). Investigative journalists comprise the most exposed group because of the inherent dangers that conducting investigations into sensible topics and contexts brings. Due to their reliance on confidential sources and whistleblowers and their explicit "watchdog " role in societies, investigative reporters are at a greater risk when it comes to potential Internet surveillance tactics and threats (Posetti, 2018). Digital and physical threats against reporters are daily realities in countries that perform poorly in regard to press freedom, but instances of attacks against reporters on the Internet now also occur with increased frequency in democratic Europe, as denounced by the Council of Europe's (2020) Platform for the Protection of Journalists. The aim of this paper is to contribute to the understanding of how investigative journalists conceptualize Internet surveillance and its related threats and what their views and remarks are regarding the impacts on their work. Methodologically, the paper is based on a thematic analysis (Braun & Clarke, 2006) of the most prominent themes emerging from a series of interviews with a sample of investigative reporters affiliated with the International Consortium of Investigative Journalists (ICIJ) and based in six European countries. Overall, this exploratory paper offers answers to the following research question (RQ):

RQ1: How is Internet surveillance perceived by European investigative journalists?

Journalism and Internet surveillance: An existential threat

Especially in the wake of the Snowden revelations in 2013, a crucial debate around the impact of Internet surveillance on journalism started (Bell & Owen, 2017; Russell et al., 2017; Thorsen,

2019). This tension is visible in the fact that the relation between journalism and surveillance is usually framed using the “chilling effects ”metaphor (Bradshaw, 2017; Eide, 2019), a figure of speech that clearly explains how comprehensively surveillance may interfere with speech at various levels (Penney, 2017). In particular, when it comes to journalists ’work, surveillance may disrupt one of the most crucial principles and moral imperatives of protection: source protection. The uncertainty about the scope of surveillance on the Internet or the possibility of having their communication wiretapped could make sources less willing to speak to reporters, jeopardizing journalists ’access to source materials, undermining their ability to carry out investigations, and even making “reporting both slower and less fruitful ”(Human Rights Watch & American Civil Liberties Union, 2014, p. 22). Journalists themselves tend to refer to surveillance in terms of the “chilling effect ”metaphor, as shown by the research about the “Snowden effect ”on journalism and journalists ’views on the issue (Wahl-Jorgensen et al., 2017). Despite the topicality of Internet surveillance and the growing evidence on how frequently journalists become targets (Butini, 2020; Committee to Protect Journalists, 2019), research about journalists ’awareness of the matter has so far produced different results or has shown how journalists sometimes tend to downplay the problem (Henrichsen, 2019). For instance, research conducted in the US illustrates how the majority of investigative reporters are certain that their data have been somehow gathered by the government (Pew Research Center, 2015). However, in the UK, regional reporters tend to play down surveillance, framing it as an issue that does not affect their work in a direct way (Bradshaw, 2017). In his study on journalists ’experiences of being under surveillance in liberal and non-liberal democracies and in non-democracies, Mills (2018) has found how concerns about surveillance tend to be correlated with journalists ’beats; those involved with “national security, terrorism, surveillance, intelligence agencies and organised crime ”tend to share a higher degree of preoccupation than those covering less controversial issues (p. 704). In the African context, journalists have expressed a systemic fear about various forms of surveillance, denouncing how the introduction of news surveillance powers makes their work more difficult and dangerous (Munoriyarwa & Chiumbu, 2020). Despite national and contextual differences among journalists regarding the perceived impact of surveillance on news work, source protection is generally indicated as the most endangered journalistic principle (Coll, 2017; Kleberg, 2015). In particular, Waters has investigated how journalists in various countries have changed their relations with sources “under a real or perceived threat of mass surveillance ”(2018, p. 1294), a topic that has also emerged clearly from the UK (Bradshaw, 2017; Lashmar, 2017). The need to find ways to effectively safeguard sources on the Internet has also inspired new

technological solutions, based on strong encryption. For instance, a growing number of whistle-blowing platforms have appeared internationally to solicit and address whistleblowers 'complaints and leaks with stronger security safeguards (Di Salvo, 2020). Nonetheless, technological solutions for spying on journalists are varied and growing, posing new threats as spying technology becomes ubiquitous and, with the use of spyware, almost impossible to track (Earp, 2021).

Surveillance practices on the Internet: A brief overview

This article is grounded in Mills '(2018, p. 690) definition of surveillance as "a set of tactics and practices with a regulatory effect on the conditions under which information is produced for public consumption. "In particular, this paper focuses on how Internet surveillance could affect the work of investigative reporters in Europe. Surveillance on the Internet occurs in a variety of forms and through the application of a series of technologies and practices, some of which may cause interference with how journalists collect, store, and communicate information to the public. According to Lyon (2015), there are at least three dimensions of contemporary Internet surveillance: 1) interception of data-in-transit via Internet cables, 2) access to stored data, and 3) installation of malware and other hacking tools to obtain access to individual computers or hardware. All three dimensions pose serious threats to the work of investigative journalists, particularly in a) their communication with one another, b) their communication with sources, and c) the data that they store to produce their journalism (Mills & Sarikakis, 2016, p. 1). The first two layers of surveillance proposed by Lyon–s (2015, pp. 8'12) taxonomy reflect powers or technical capabilities that require resources that only the state and intelligence services have (of which the Snowden revelations have provided overwhelming evidence). On the contrary, various corporate and private actors can now engage in attacks against investigative reporters, aiming to gain remote access to their devices or archives. This is possible with spyware, whose diffusion is becoming commodified as its commercial availability is growing steadily (Harkin et al., 2020). Growing evidence of state actors 'and large companies 'use of such tactics to target journalists has surfaced around the globe, including in Europe (Datta, 2020). For instance, a major case emerged in Germany in 2017, when it was revealed that German intelligence services spied on international journalists 'communication for years (Baumgärtner et al., 2017). Similar concerns have recently been raised in Poland (Liven & Trytko, 2017) and the UK (Fitzgibbon & Boland-Rudder, 2014; Jones, 2019), among others. In 2020, the partner organizations of the Council of Europe's Platform to Promote the Protection of Journalism and Safety of Journalists, in its own annual report, denounced the overall expansion of Internet surveillance powers in Europe as a problematic aspect of journalists 'work. In particular, the report pointed at France, Switzerland,

Spain, the Netherlands, Slovenia, and Poland as the most controversial cases (Council of Europe, 2020). Parallel to these purely technical threats, journalists are also increasingly targeted with social engineering practices aimed at obtaining their personal information or account details. Phishing, a practice that brings together social engineering and technical hacking, is defined as “the impersonation of a legitimate source to acquire confidential information ”and can occur via email, instant messaging, or Voice over Internet Protocol (VoIP) (Aldawood & Skinner, 2018, p. 63) or by exploiting vulnerabilities in popular apps and mobile operating systems. Evidence about journalists targeted in this way is growing, and the tactics involved can be extremely tailored to journalists, who may be contacted by hackers impersonating colleagues or other media personalities (Satter & Bing, 2020).

Information security in journalism: A still nascent field of research

Technology offers journalists some solutions to the threats posed by Internet surveillance. In particular, software based on strong encryption standards (e.g., Signal, SecureDrop, GlobaLeaks, or the Tor Browser) is becoming a crucial solution in terms of privacy protection and anti-surveillance safeguards, especially for investigative reporters, serving as a vital tool to protect press freedom (Tsui, 2019). Information security in journalism is still an understudied field that only recently has started to produce literature about how and why journalists adopt stronger and safer communication strategies in the context of their work (Taylor, 2015; Tsui & Lee, 2019). Nevertheless, the limited existing literature tends to confirm the importance of information security practices and tools, while illustrating various barriers to and limitations in the adoption of such technologies. For instance, McGregor et al. (2015) have focused on journalists ’practices and needs in terms of “computer security ”in France and the US, underlying the existence of a digital divide between reporters and their sources. Other research has focused on the frictions between individual journalists ’and organizations ’concerns about information security (McGregor et al., 2016). Research in this area has also paid attention to information security’s role in coordinating internal communication in collaborative investigative projects, such as the ”Panama Papers“(McGregor et al., 2017). Moreover, the aforementioned research conducted in the US in 2015 has shown that despite investigative journalists ’awareness of the risks of Internet surveillance, only a minority of them uses security tools in the context of news work (Pew Research Center, 2015). Similarly, journalists ’overall poor understanding of how secure communication systems work has been confirmed in the US and in Europe (McGregor & Watkins, 2016). Analyzing journalists ’responses to information security, Henrichsen has focused on the

barriers preventing the adoption of information security in US newsrooms and has found five different patterns, “varying from the lack of usable tools to structural and cultural reasons ”(2019, p. 333). Analyzing journalists ’attitudes toward security in Hong Kong, Tsui and Lee have stressed the differences between journalists with ”novice“and “advanced ”security mindsets, which directly affect their likelihood to critically use their digital freedoms (2019, p. 13). Besides these few studies about how journalists conceptualize and use information security tools, encryption and information security are generally mentioned in articles dealing with related issues, such as whistleblowing and source protection or surveillance and the Snowden case aftermath. For instance, the aforementioned literature about source protection in this surveillance age usually refers to information security as a necessity (Ananny, 2018, pp. 152–155). Moreover, communication tools grounded in strong encryption are usually connected to the practice of facilitating whistleblowing on the Internet (Bosua et al., 2014; Di Salvo, 2020; Dreyfus et al., 2013). Overall, the available literature still lacks a European view of how journalists conceptualize Internet surveillance. Although this explorative article does not provide conclusive results about the European state of affairs in this field, it attempts to fill this gap in scholarly research by presenting first-hand findings obtained from journalists working in the ICIJ, one of the most advanced international investigative reporting organizations.

Methodology and sampling

This article is based on six semi-structured interviews with a sample of European investigative reporters, conducted via Voice over Internet Protocol (VoIP) during the spring of 2020. The interviewees were chosen among the ICIJ members based in six countries: Italy, Germany, Hungary, Spain, Switzerland, and the UK. The decision to consult solely ICIJ members was motivated by two factors: 1) the need for a consistent sample of journalists, composed of individuals working in international investigative projects but located in different European countries and with different journalistic cultures, and 2) the opportunity to discuss the issues at the core of this article with journalists involved in one of the most prestigious and important cross-border institutions of today’s investigative journalism, also responsible for some of the most impactful investigations in recent times, including the ”Panama Papers“and the ”Offshore Leaks“series. The interviews were first transcribed by using the automated software Sonix.ai and later cross-checked and amended manually by the author. The interviews with the German, Hungarian, and UK journalists were conducted in English, while those with the Italian, Spanish, and Swiss journalists, who had a good command of Italian (the author’s native language ,(were conducted in that language. Later, the interview transcripts were analyzed by means of a thematic analysis to

identify recurring themes in the journalists 'responses, following an inductive approach (Braun & Clarke, 2006, p. 83). Intended here as the most salient constellations of meanings present in the interview transcripts (Joffe, 2012, p. 209), the themes were grouped under broader categories, based on their recurrence in the interviewees 'responses. Among all the ICIJ members listed on the organization's website, the journalists in the sample were chosen for their familiarity with covering Internet surveillance or other related issues or for their experience with the use of encryption tools, when visible in their bios or Twitter profiles. Given the sensitivity of the topics covered by this article, the interviewees were granted anonymity, and all details that could identify them from the quotes included in the Results section were removed. Moreover, for security reasons, the interviews did not cover details of any ongoing or past investigations or projects undertaken by the interviewees, for the sake of source protection.

Results: how European journalists see digital surveillance

Five prominent recurring themes emerge from the interviews. These are 1) source protection under stress (together with data storage and communication among peers and colleagues), 2) the ephemeral nature of Internet surveillance and the uncertainty about being a potential target, 3) the (private) expansion of Internet surveillance, 4) the international networks of Internet surveillance and the dangers of intelligence sharing, and 5) phishing and the dangers of "clicking on the wrong link. "Two other themes emerge from individual journalists or are shared by a minority of them, but they indicate other crucial insights about the danger of surveillance. These are 6) the need to adjust countersurveillance practices, depending on the perceived threat level, and 7) a pessimistic perspective on the effectiveness of information security strategies. These themes express the dangers and the concerns that the interviewed investigative journalists consider as alarming when asked to elaborate on how, where, and by whose action Internet surveillance could interfere with their news work. The themes either expose critical characteristics of contemporary Internet surveillance and its peculiarities or express their explicit abusive nature in regard to journalistic practices and principles.

1) *Source protection under stress (together with data storage and communication among peers and colleagues)*

Interviewed journalists agree that source protection is the element of news work that is the most endangered by Internet surveillance. All interviewed journalists express similar views on the matter by citing their preoccupation with having an actual possibility to effectively protect their

sources or seeing them exposed by means of Internet surveillance. This theme emerges spontaneously as the first or core argument of the journalists' reasoning. Source protection is also frequently mentioned in connection with the use of encryption tools or with the need for securely stored data and secure communication with colleagues and peers. Moreover, as pointed out by the Hungarian journalist, meeting sources in person is still considered more secure than online communication, where ensuring that all parts involved are not under some kind of surveillance is more difficult. The work conditions imposed by the COVID-19 pandemic have also exacerbated this situation.

> Basically, we need to be careful about how we communicate with each other and with our colleagues, when we talk about sensitive stories and, even more importantly, sensitive sources. Basically, we don't talk about our sources. We use encrypted channels and certain applications—among which, Signal is the most widely used. Even there, we don't talk about and we don't discuss our sources. The other point is how to communicate with sources.
> (Hungarian journalist)

For others, it is almost impossible to separate source protection from other parts of news work, as they are considered interconnected and consequently, have to be assessed in a collective way. In particular, even the initial stage of an investigation—research—could expose journalists and their sources, as digital devices may open the door to surveillance.

> All these are very delicate phases, but the first one, research, especially when done in a collaborative way, is a moment of potential weakness, where journalists work in isolation and electronic devices may become the entrance doors for surveillance. Every computer is a potential liability because each access point could be the one that would compromise the whole network. Research is a very important phase of an investigation because months of work could be at risk. Then there's everything in regard to communicating with sources and protecting the meetings and contacts by using encrypted chatting apps or leaking platforms or any other tool capable of safeguarding both sides, who can be harmful to each other.
> (Italian journalist)

In particular, secure encrypted data storage is mentioned in the context of source protection, as another crucial element of protecting journalistic work from Internet surveillance.

> It's not only about communications, but it's also a matter of how you store your data. That's of course also very important—using encryption on your devices and anywhere else.

(Hungarian journalist)

A similar concern about how materials and data are archived is mentioned as a parallel element needed for effective source protection.

> The protection of the materials and data that I archive is crucial, too. Recently, I've learned how to use an encrypted hard drive and how important it can be. But the most immediate thing is definitely the protection of sources and their anonymity.
> (Spanish journalist)

Other journalists have also highlighted the fact that living in a democracy does not pose immediate and tangible threats compared with the situation in nondemocratic states, for example:

> In Spain, we have problems, but we're not under a dictatorship, and we don't face problems as severe as those in other countries. The most important aspect is definitely source protection and the fact that they don't feel protected enough, maybe also because of previous bad experiences with the media.
> (Spanish journalist)

2) The ephemeral nature of Internet surveillance and the uncertainty about being a potential target

The necessity of assessing a journalist's own threat model is also connected to the difficulties in effectively verifying whether they have been or are potential targets of surveillance. The reasons for this uncertainty emerge from different areas, either technical (connected to the nature of the agents of Internet surveillance) or the weaknesses and potential loopholes of national regulations. For some interviewed journalists, this results in adapting their work practices and routines as if they are subjected to constant surveillance, starting from the assumption that someone is listening. For instance, the Swiss journalist declares:

> Investigative reporters comprise a category particularly at risk. The problem is that you cannot really tell if you are a target. Sure, you could have your computer forensically checked, but it is really difficult to be sure that your device is not compromised. You need to adapt to the situation, but I think it is not by chance if people dealing with these issues never carry their computer with them or always encrypt their devices. You need to start from the assumption that you're subject to

total surveillance.
(Swiss journalist)

For others, even when legal safeguards or various checks and balances are in place and guaranteed, some tension is always unresolved, as the ways in which the surveillance of a journalistic source could be operated vary and are sometimes applied with limited transparency, even when and where democratic standards are in place. Even in contexts where democratic checks and balances on surveillance are available, journalists should not exclude the possibility that their communication may be subject to surveillance.

> There is, of course, the possibility that surveillance may be authorized and passed through the checks and balances. Therefore, the tension is still there. I would say that safeguards are far more comprehensive and real in a way [that they] never [were] in the '80s. Is it enough for journalists to do anything differently? No. Is it enough for journalists to sleep happily in their beds? Yes. But not to change practices.
> (UK journalist)

The assumption of being the target of some forms of surveillance is sometimes held even in the absence of evidence. This is not connected to a paranoid attitude but to the need to offer sources the strongest possible safeguards.

> In Hungary, we operate under the assumption that we can be under surveillance. But I never saw any evidence of actually being speaking under surveillance. I never felt like that. If they [the government] do it, then they keep their information to themselves. I never heard from sources that they got burned. We have to be careful, of course, but I'd like to think that they have better things to do than monitor us.
> (Hungarian journalist)

The reasons for this perceived uncertainty about the possibility of being put under surveillance are also connected to the potential unknown actors with surveillance capabilities that may engage in these operations against journalists. These actors 'lack of transparency leads to concerns. For instance, in Italy, some surveillance companies have been involved in controversies about the use of their products in non-transparent if not abusive ways.

> We know very well that Italy is a major exporter of dual-use technology, and some recent cases

> have shown that interception software programs used by courts are tendered to companies that also operate in a commercial for-profit market. This may lead us to think that our communications may also be monitored in the same way. There is always a question mark.
> (Italian journalist)

3) The (private) expansion of Internet surveillance

The expansion of today's potential actors who may conduct surveillance operations against journalists on the Internet has also been discussed. For the sample of journalists, state actors are not considered the sole potential threats, since powerful private companies now have access to technologies for conducting unauthorized Internet surveillance, due to the expansion of the massively unregulated surveillance market. This theme has emerged in relation to large investigations into offshore economies and corporate misbehavior, such as those revealed in the ".Panama Papers"In particular, private companies producing spyware technologies are indicated as potential threats. For instance, the German journalist points to the fact that currently, private actors may have access to surveillance technologies that were previously only available to state actors. This thus increases the number of actors that may potentially hold the resources to monitor journalists investigating them, even in Europe, where journalists working on major international investigations have been killed.

> There are means and ways to surveil people via private companies like [the] Niv, Shalev and Omri (NSO) Group that may be used by other actors, too. And then if you look at the cases of Daphne Caruana Galizia in Malta and Ján Kuciak in Slovakia, you clearly see that investigative journalists who investigate financial crimes could get killed inside the European Union, too. Both of them have worked on the ".Panama Papers"So, I'm a little wary here, and I see this as a big problem.
> (German journalist)

In Spain, specific evidence has emerged about national instances of private actors conducting various forms of surveillance that target journalists covering large corporations. This was a major turning point in Spain, as many journalists had to reckon that the surveillance dangers in the country might be more widespread than those expected, again involving more potential actors.

> That was a moment of reckoning when journalists realized that some companies might actually

> have more power than the state if they want to interfere with journalists 'work. [...] I never had personal experiences of surveillance, but I know of a colleague who had been surveilled by a private company while he was investigating its businesses. He had no idea about it until he was called to testify. He had his phone tapped for six or seven months.
> (Spanish journalist)

Private actors have been referred to as among the most powerful players in today's Internet surveillance at the international level, a state of things reinforced also by the nature and geopolitics of the contemporary Internet. This point has been connected to private intelligence merchants and large corporations hiring surveillance companies, now to be included with state actors as among the best equipped players with surveillance capabilities, a sea change in the relation between journalists and surveillance.

> The point is now that the Internet is extraterritorial, so you also get highly competent, large American corporations [that] may use outposts in low regulation areas to mount computer exploitation attacks. And journalists will be targeted, and they are targeted. The major players— and this is new—do not now just include major international intelligence agencies but also private-for-hire groups offering similar skills. So, three classes: the national intelligence agencies, the private intelligence merchants, and the particular corporations [that] may have access for individual reasons.
> (UK journalist)

4) The international networks of Internet surveillance and the dangers of intelligence sharing

Overall, more concerns were raised in regards to state and private surveillance at the international level rather than the national one. The role of "intelligence-sharing agreements "among countries (Kim et al., 2018) has been discussed as the most problematic layer of international surveillance by state actors. Whereas interviewed journalists overall tend not to fear surveillance by the state agencies of their own countries, they fear that intelligence-sharing agreements among countries may expose their communications or those of their colleagues, especially in cases of international journalistic cooperation, such as cross-border investigations (Leigh, 2019, pp. 127–154, 197–199). The Swiss journalist expresses clear views on this potential threat:

> If you work with international journalistic organizations, you also work with colleagues who live in

> way more dangerous contexts than yours. We know that there's friendship among secret services, so one of my communications that gets intercepted may not expose me to any risk, but it could be handed over to the secret services in Azerbaijan or another complex country. And this may bring serious troubles to someone else.
> (Swiss journalist)

These concerns are triggered by the fact that intelligence agencies are usually not allowed to spy within the national borders of their countries but may have the opportunity to intercept and wiretap international communications that could be shared among allied agencies. A recent court case in Germany has provided evidence of this practice.

> The Secret Service is not allowed to surveil German journalists, but they are allowed to surveil foreign journalists. What are they doing with this information? So, when they are surveilling, for example, a journalist from Afghanistan, are they sharing the information with the Secret Services from Afghanistan because they want to [receive] a favor in return? Or are they sharing with the Americans because they have cooperation, or are they sharing it with the French guys because they have an open line to them or whatever? There's a cold case right now in Germany, and they're trying to stop the German Secret Service from spying on foreign journalists. Do I think that we are in danger, that we might be surveilled by the Secret Service in Germany? I don't think so. I'd say they usually stick to their rules.
> (German journalist)

5) Phishing and the dangers of "clicking on the wrong link

The interviewed journalists express utmost concerns regarding digital threats by referring to "phishing "as the potentially most dangerous attack strategy against their digital devices. Phishing emails can also be a strategy to install spyware software on targets 'devices in order to gain remote access. Recent research has shown how phishing is becoming an increasingly common digital attack strategy against journalists (Amnesty International, 2019; Henrichsen, 2020). The growing sophistication and customization of this tactic was also mentioned. Now, phishing emails aimed at attacking journalists can be produced in a blatant way, frequently with the use of texts faking academic requests, an element that clearly shows the social engineering involved in phishing.

> For instance, we receive emails from contacts impersonating students or academics asking us for interviews for their theses or research. They usually come from countries where you may ask

> yourself how they even got your name. After some initial emails, they send you a malicious link to click on. This happened to me, and it contained malware. You need to find a technique to understand if a person is genuine or not.
> (Italian journalist)

Besides phishing emails and fake attachments, popular communication apps, including WhatsApp, could also become access points for phishing attacks. According to the Swiss journalist, this may expose less digital-savvy journalists to more risks as the attack may be launched in a mundane context or in situations where they may lower their security mindset and mistakenly feel safe.

> What I fear the most is leaving my computer unattended, so I always carry it with me. Also, I'm more scared about my iPhone because even when you use all the palliative measures, it is still a dangerous tool. WhatsApp is a problem because it is known that this app has been exploited to gain access to journalists 'phones. Other apps may pose the same threats.
> (Swiss journalist)

Fears of undetectable phishing attacks and malware remote implantation are indicated as reasons for changing habits regarding information security and digital hygiene.

> I think phishing is a big danger because it is enough to not be focused for a second and click on the wrong link. Meanwhile, now there are even emails that you don't even have to click on. It's enough that you're receiving them. I think the same is possible with texts that someone could send you with you even noticing them, but your phone gets infected anyway. Honestly, we have to act like our devices are already infected if we want to be really secure. So, what we do from time to time, when we think that it's getting really, really dangerous, is go out, buy new phones and new SIM cards. We do all this stuff because we know it could be already too late for the devices that we are using.
> (German journalist)

In the case of phishing attacks, potential adversaries mentioned by the journalists include both state actors and private companies that may use phishing to target journalists.

> There were more recent stories, like the one about Black Cube, this company that created false identities for other organizations or clients. Another lesson that we learned about [concerned] John Podesta's emails and the Clinton campaign and how they got hacked—it all started with

> very simple phishing operations. So, the problem with that is that once you click on the wrong link, you get screwed.
> (Hungarian journalist)

Phishing is also a tactic that could jeopardize any other information security strategy because when a device is compromised by malware, any encryption-based strategy has to be considered completely pointless.

> If someone gets into your phone, then it doesn't matter anymore if you are encrypting the messages because they can basically read what you're typing in real time. So there [are] a number of problems within surveillance. And we know how the big international secret services hate that they can't get into Pretty Good Privacy (PGP) or Signal. And we know that they at least have one door into Signal by conducting surveillance on the whole phone, for instance. So there may be a day when we are sure we're communicating securely, but in reality, we don .t'
> (German journalist)

It should also be mentioned in this context that some spyware software can be installed on a target's device with what is defined as a "zero click "exploit. In these cases, spyware software is installed without requiring any action by the target, who doesn't even have to click on a link in order to be infected. This has emerged with alarming evidene with the "Pegasus Project "investigation into the Pegasus spyware, which operates in this fashion (Rueckert(2021 ,. Interviews included in this article were conducted before the publication of the "Pegasus Project "investigation.

6) Adjusting counter-surveillance practices, depending on perceived threat level

Whereas source protection is always on top of journalists 'concerns, as emerged from the interviews,some of them have also pointed out that the beat, the nature of the sources, and the topic of reporting make a direct difference in calibrating the danger of surveillance and consequently, the threat model that journalists will have to face.

> It is not ubiquitous that you would have that concern. An example I would always give is where you have medical whistleblowers. So, for example, I've done several investigations where a doctor or a clinician with material, some of which they shouldn't have given to me, reveals gross misconduct by others and by their institution. That person is clearly putting their professional standing

> in line, leading to great risk. And I have to protect them to the utmost. But in those contexts, I would not feel any anxiety about interception on the Internet. The ability to intercept the Internet is, with almost no exception, in my experience, limited to nation-state actors and only the intelligence or police functions of the nation state [that] will, in any reasonably governed state, only act according to the rule of national law. Now, that may allow them far more powers than the ordinary citizen or legislature was told about, but they have other jobs. They are not out there to surveil everyone on everything all the time.
> (UK journalist)

The nature of the investigations and the sensitivity of the sources and source materials involved are considered crucial factors in pushing for the adoption of higher standards of security and source protection compared with other, less sensitive, scenarios.

> If you have something that is sensitive by nature because it has been leaked to you or because you have got a strong confidential source, then of course you have to be more careful and aware of the risks.
> (Hungarian journalist)

Working on international collaborative projects in the context of the ICIJ activities also means raising their security protocols to higher standards, given the sensitivity of the materials and the work that such collaborations usually entail.

> When I work with the ICIJ, there's a shift to a higher level of security. For instance, we use document-sharing platforms that have been created in-house and adopt higher standards of security, such as two-step verification.
> (Spanish journalist)

7) A pessimistic perspective on the effectiveness of information security strategies

Despite being aware that information security plays a fundamental part in securing investigative journalists 'work and sources, interviewees have expressed some very pessimistic views on the effectiveness of information security in the fight against pervasive surveillance, even referring to digital strategies as mere "palliative measures "sometimes. According to these views,, the highest level of information security in a journalistic context may pass through not using electronic devices at all.

> There is no such thing as digital security. […] The more you become advanced in using secure tools, the more you lose in terms of usability. This is a big problem because not all investigative reporters are digital natives or good at computing. At the end of the day, it is all a bit futile. Resistance is futile. I have been using Pretty Good Privacy (PGP) for twenty years now, and I have come to the conclusion that all these are palliative measures.
> (Swiss journalist)

Whereas older software, such as the aforementioned PGP, certainly pose challenges in terms of usability, given their lack of user friendliness, it should also be noted that more recent software, such as mobile chatting apps like Signal, have decisively made access to and usage of safer communication tools easier for both journalists and the general public (Gallagher, 2021). Overall, a general feeling of uneasiness regarding the use of digital tools has emerged from the interviews, especially in light of how digital devices may become entry points for various types of surveillance. In particular, one journalist stresses the point that by design and because of the ubiquitousness of data gathering and exploitation, digital software may become natural "tools for interception."

> The moment I turn on my computer or switch on my mobile phone or any other digital tool in the room, it is already a red flag because all these devices could be potential tools for interception, even when switched off or non-active.
> (Italian journalist)

Discussion: European takes on the impact of surveillance on journalists

The views expressed by this sample ofEuropean ICIJ-affiliated journalists show various themes about the impact of Internet surveillance on journalism, signaling the existence of an urgent problem facing journalists 'security across Europe. The interviewed ICIJ-affiliated European investigative reporters share concerns about being subjected to various potential forms of Internet surveillance. In particular, uncertainty and lack of transparency appear to be the most powerful reasons for concern. According to the journalists interviewed for this article, this is mostly due to the general obscurity of some players in Internet surveillance (mainly state actors and intelligence agencies), the invisibility of their tactics, the potential abusive nature of certain forms of monitoring, or the unlawful basis of others, starting from those applied by powerful private actors. This uncertainty results in a perceived need for working as if surveillance was a constant and pressing threat, especially in terms of communicating with sources and colleagues and storing data. This is definitely one of those "chilling effects "of Internet surveillance that research

conducted in both democratic and non-democratic contexts has underlined, especially in psychological terms (Mills, 2018). Interestingly, the interviewed journalists tend to consider Internet surveillance as a problem even when they clearly state that there are few reasons for worrying in their home countries, especially regarding the actions of their countries ’intelligence agencies. In particular, they tend to exclude the possibility that national intelligence agencies may conduct direct surveillance on them or their work, while fearing that foreign agencies may instead have an interest. This is reflected by the methods and structures of contemporary investigative journalism—and of the ICIJ in particular—and cross-border investigations. For the interviewed journalists, this results in a shared sense of responsibility toward colleagues and peers and in the consequent adoption of communication safeguards and strategies that would be overreaching in other contexts.

In the interviewed journalists ’views, surveillance by state actors is strictly connected to the chosen topic of coverage and beat. According to the results of this study, only those journalists covering national security, intelligence agencies, and other high-ranking sensitive issues may in effect become targets of such surveillance. Others, even when conducting investigations in other fields, may not have a legitimate direct concern of this kind. These results confirm those of previous studies, where a similar attitude emerged in connection to reporting about national security, terrorism, or organized crime (Mills, 2018). Likewise, this also emerged in the “security by obscurity ”framework proposed by McGregor and Watkins (2016), where the sensitivity of the journalistic work or the topics covered is perceived as a proxy for a more tangible exposure to potential Internet surveillance. Moreover, the results of this study echo those of previous studies, where journalists ’beats appear to “strongly influence how journalists perceive and value information security ”(Crete-Nishihata et al., 2020, p. 16). Whereas this idea is expressed mostly about state actors, malicious monitoring by private entities raises a completely different layer of concern among the interviewed journalists. Some of them point to the overall lack of regulations for the surveillance software market and the exponential growth of sophisticated digital and social engineering attacks, starting from phishing tactics, that are progressively being commodified. Phishing and spyware overallare interesting case studies for journalists ’safety, since they both have the ability to jeopardize any other information security strategy by simply letting the attacker gain remote access to a device by using dedicated malware or spyware software. More research in the future should be addressed to the profound implications that the use of such intrusive technology can have on journalists ’freedoms and safety.

Conclusions: the dangers and uncertainties of surveillance invisibility

What emerges from this research article is a shared sense of need for protection from surveillance among journalists, an outcome that is again in line with the findings of previous research conducted in the US (Henrichsen, 2019). This sense of feeling in need of protection is the result of different factors, varying from personal experience of surveillance to paranoia or a sort of "sublime surveillance "that causes unjustified fears, but it definitely reinforces once more the existence of those "chilling effects "of surveillance on journalists, even in democratic countries and "safe "contexts. Overall, to emerge from this article's results is a view of surveillance that appears in line with the "black box "metaphor (Pasquale, 2015), where surveillance is perceived as a constant, taken-for-granted threat, but whose inner mechanisms, effectiveness, and effects on journalists 'practices and safety remain obscure because of contemporary surveillance's inner elusiveness and multiform nature. Whereas source protection appears as the topic of utmost urgency,pessimistic views about the effectiveness of information security leave many questions open, especially when it comes to whether the aforementioned need for protection may actually be fulfilled. This point is even more crucial in the wake of the "Pegasus Project "revelations which showed with strength how even the most sophisticated information security practices can become useless in scenarios where spyware technology is involved. Thus, the results of this research - and those of research in this area overall - have to be read in an ambivalent way: undoubtedly, it is fundamental to push for more information security awareness in journalism and for more knowledge sharing and training among journalists. Similarly, to adopt information security practices and software is a must for contemporary journalism, as these practices offer protection towards some forms of Internet surveillance, especially in regards to protecting communications. Yet, even with adopting the most advanced and secure solutions and safeguards, doubts and uncertainty will always be present, as surveillance technology, their producers and users seem to have the capacity of being constantly one step ahead in what looks increasingly as a severe power imbalance. This makes those journalists who are the most encryption-savvy paradoxically also the most exposed to these fears, as journalists covering sensible beats such as national security will also be exposed to the most advanced forms of surveillance, starting from spyware. In the long run, this sense of uncertainty may impact severly on the security and well-being of investigative journalists, who may find themselves lost in a rabbit hole of fear and insecurity whose outcome could be self-censorship and silence.

These findings emerge from a limited study that is clearly not generalizable for a complete understanding of how investigative reporters in Europe conceptualize Internet surveillance. The

interviewed journalists represent different genders, generations, and backgrounds, with varying experiences and competencies in information security, but they are still all part of one, global, highly advanced elite organization of today's investigative journalism (the ICIJ), one that may fit under the label of "pioneer journalism "for cross-border investigations (Hepp & Loosen, 2019). Despite its limitations, this paper offers insights for the expansion of the understanding of information security in journalism. Consequently, further research into this fundamental topic would definitely require a more quantitative and horizontal approach in order to gain a more in-depth understanding of the impact of surveillance on European journalism. Nonetheless, these explorative results also bring insights about how post-Snowden investigative journalism is taking shape in terms of fighting surveillance and its perils and about who its enemies could be.

References:

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), IEEE, 62.68–

Amnesty International. (2019). Evolving phishing attacks targeting journalists and human rights defenders from the Middle-East and North Africa. https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/ .

Ananny, M. (2018). Networked Press Freedom. Creating Infrastructures for a Public Right to Hear. Cambridge, MA: The MIT Press.

Anesi, C., & Angius, R. (2020, June 22). Sorveglianza: Giornalisti ancora nel mirino dei software spia. IRPI Media. https://irpimedia.irpi.eu/spyware-pegasus-marocco/ .

Baumgärtner, M., Knobbe, M., & Schindler, J. (2017, February 24). Documents indicate Germany spied on foreign journalists. *Der Spiegel* .https://www.spiegel.de/international/germany/german-intelligence-spied-on-foreign-journalists-for-years-a-1136188.html .

Bell, E., & Owen, T. (2017). Journalism after Snowden. The future of the free press in the surveillance state. Columbia University Press.

Bosua, R., Milton, S., Dreyfus, S., & Lederman, R. (2014). Going public: Researching external whistleblowing in a new media age. In A. J. Brown (Ed.), International handbook on whistleblowing research (pp. 250–272). Edward Elgar Publishing.

Bradshaw, P. (2017). Chilling effect: Regional journalists 'source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations. Digital Journalism, 5(3), 334.352–

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77.101–

Butini, C. (2020, March 13). An international case against surveillance of reporters. Columbia Journalism Review. https://www.cjr.org/analysis/bnd-surveillance-press-freedom.php

Citizen Lab. (2019). NSO Group / Q cyber technologies. Over one hundred new abuse cases. https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

Coleman, G. (2017). The public interest hack. Limn, 8, 18.23–

Coleman, G. (2019). How has the fight for anonymity and privacy advanced since Snowden's whistle-blowing? Media, Culture & Society, 41(4), 565.571–

Coll, S. (2017). Source protection in the age of surveillance. In E. Bell & T. Owen (Eds.), Journalism after Snowden: The future of the free press (pp. 85–96). Columbia University Press.

Committee to Protect Journalists. (2019). UK report shows surveillance efforts involving journalists. https://cpj.org/2020/03/uk-report-shows-surveillance-efforts-in/

Council of Europe. (2020). Attacks on media in Europe must not become a new normal. https://www.coe.int/en/web/media-freedom/-/annual-report

Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L., & Deibert, R. (2020). The information security cultures of journalism. Digital Journalism. https://doi.org/10.1080/21670811.2020.1777882

Datta, A. (2020, February 17). Governments of the world just ramped up spying on reporters. Columbia Journalism Review. https://www.cjr.org/first_person/ft-nations-surveillance-attacks.php

Di Salvo, P. (2020). Digital whistleblowing platforms in journalism. Encrypting leaks. Palgrave Macmillan.

Dreyfus, S., Lederman, R., Brown, A. J., Milton, S., Miceli, M. P., Bousa, R., Clausen, A., & Schanzle, J. (2013). Human sources: The journalist and the whistleblower in the digital era. In S. Tanner & N. Richardson (Eds.), Journalism research and investigation in a digital world (pp. 48.Oxford University Press Australia & New Zealand .(61–

.Earp, M. (2021)Pegasus Project revelations show added layer of risk for corruption reporters. The Committee to Protect Journalists, July 30th. https://cpj.org/2021/07/pegasus-project-risk-corruption-reporters/ .

Eide, E. (2019). Chilling effects on free expression: Surveillance, threats and harassment. In R. Krøvel & M. Thowsen (Eds.), Making transparency possible. An interdisciplinary dialogue (pp. 227.Cappelen Damm Akademisk .(242–

El Confidential. (2019, June 18). Villarejo espi óa El Confidencial y las llamadas de varios de sus periodistas. El Confidential. https://www.elconfidencial.com/espana/2019-06-18/espionaje-comisario-villarejo-periodistas-elconfidencial-llamadas_2077270/

European Federation of Journalists. (2020). Victory for press freedom in Germany: Global mass surveillance ruled unconstitutional. https://europeanjournalists.org/blog/2020/05/19/victory-for-press-freedom-in-germany-global-mass-surveillance-ruled-unconstitutional/ .

Farrow, R. (2019, October 7). The Black Cube Chronicles: The private investigators. The New Yorker. https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators .

Fitzgibbon, W., & Boland-Rudder, H. (2014, September 15). Journalists hit back with anti-spying legal challenge. The International Consortium of Investigative Journalists. https://www.icij.org/inside-icij/2014/09/journalists-hit-back-anti-spying-legal-challenge/.

Franceschi-Bicchierai, L. (2016, October 20). How hackers broke into John Podesta and Colin Powell's Gmail accounts. Motherboard. https://www.vice.com/en_us/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts .

Gallagher, R. (2021, May 28). Signal jabs at Facebook and navigates growing pains as popularity surges. Bloomberg News. https://www.bloomberg.com/news/articles/2021-05-28/signal-app-is-surging-in-popularity-and-hitting-growing-pains .

Harkin, D., Molnar, A., & Vowles, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. Crime Media Culture, 16(1), 33.60–

Henrichsen, J. R. (2019). Breaking through the ambivalence: Journalistic responses to information security technologies. Digital Journalism, 8(3), 328.346–

Henrichsen, J. R. (2020). The rise of the security champion: Beta-testing newsroom security cultures. Tow Center for Digital Journalism. https://www.cjr.org/tow_center_reports/security-cultures-champions.php .

Hepp, A., & Loosen, W. (2019). Pioneer journalism: Conceptualizing the role of pioneer journalists and pioneer communities in the organizational re-figuration of journalism. Journalism, https://doi.org/10.1177/1464884919829277 .

Hopkins, N., & Kirchgaessner, S. (2019, October 29). WhatsApp sues Israeli firm, accusing it of hacking activists' phones. The Guardian. https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones .

Human Rights Watch & ACLU. (2014). With liberty to monitor all. How large-scale US surveillance is harming journalism, law and American democracy. https://www.aclu.org/report/liberty-monitor-all-how-large-scale-us-surveillance-harming-journalism-law-and-american .

Joffe, H. (2012). Thematic analysis. In D. Harper & A. R. Thompson (Eds.), Qualitative research methods in mental health and psychotherapy: A guide for students and practitioners (pp. 209–223). Wiley-Blackwell.

Jones, M. (2019, July 10). UK hosts press freedom summit while fighting for right to spy on media. The Bureau of Investigative Journalism. https://www.thebureauinvestigates.com/stories/2019-07-10/uk-hosts-press-freedom-summit-in-london-while-fighting-for-right-to-spy-on-media .

Kim, S., Lee, D., Lubin, A., & Perlin, P. (2018, April 23). Newly disclosed documents on the Five Eyes Alliance and what they tell us about intelligence-sharing agreements. Lawfare. https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing .

Kleberg, C. F. (2015). The death of source protection? Protecting journalists 'source in a post-Snowden age. LSE Polis. http://www.lse.ac.uk/media@lse/documents/Death-of-Source-Protection-Carl-Fridh-Kleberg.pdf .

Lashmar, P. (2017). No more sources? The impact of Snowden's revelations on journalists and their confidential sources. Journalism Practice, 11(6), 665.688–

Leigh, D. (2019). Investigative journalism. A survival guide. Palgrave Macmillan.

Liven, I., & Trytko, K. (2017, October 2). Government spying threatens media freedom in Poland. The European Journalism Observatory. https://en.ejo.ch/media-politics/government-spying-threatens-media-freedom-poland .

Lyon, D. (2001). Surveillance society. Monitoring everyday life. Open University Press.

Lyon, D. (2015). Surveillance after Snowden. Polity.

McGregor, S. E., Charters, P., Holliday, T., & Roesner, F. (2015). Investigating the computer security practices and needs of journalists. Proceedings of the 24th USENIX Security Symposium, 399.414–

McGregor, S. E., Roesner, F., & Caine, K. (2016). Individual versus organizational computer security and privacy concerns in journalism. Proceedings on Privacy Enhancing Technologies, 2016(4), 418.435–

McGregor, S. E., & Watkins, A. E. (2016). Security by obscurity: Journalists 'mental models of information security. International Symposium on Online Journalism, 6(1), 33.49–

McGregor, S. E., Watkins, A. E., Al-Ameen, M. N., Caine, K., & Rosener, F. (2017). When the weakest link is strong: Secure collaboration in the case of the Panama Papers. Proceedings of the 26th USENIX Security Symposium, 505.522–

Mills, A. (2018). Now you see me –now you don't: Journalists 'experiences with surveillance. Journalism Practice, 13(6), 690.707–

Mills, A., & Sarikakis, K. (2016). Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism. Big Data & Society, 3(2).

Minder, R. (2019, July 29). The former police commissioner rattling Spain's establishment. The New York Times. https://www.nytimes.com/2019/07/29/world/europe/spain-jose-manuel-villarejo.html .

Munoriyarwa, A., & Chiumbu, S. H. (2020). Big Brother is watching: Surveillance regulations and its effects on journalistic practices in Zimbabwe. African Journalism Studies, 40(3), 26.41–

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. Internet Policy Review, 6(2). https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case .

Pew Research Center. (2015). Investigative journalists and digital security. Perceptions of vulnerability and changes in behavior. https://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/ .

Posetti, J. (2018). The future of investigative journalism in an era of surveillance and digital privacy erosion. In O. Hahn & F. Stalph (Eds.), Digital investigative journalism. Data, visual analytics and innovative methodologies in international reporting (pp. 249.Palgrave Macmillan .(261–

Rueckert, P. (2021). Pegasus: The new global weapon for silencing journalists. Forbidden Stories, July 18th. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

Russell, A., Kunelius, R., Heikkilä, H., & Yagodin, D. (2017). Journalism and the NSA revelations: Privacy, security and the press. I.B. Tauris.

Satter, R., & Bing, C. (2020, February 5). Exclusive: Iran-linked hackers pose as journalists in email scam. Reuters. https://www.reuters.com/article/us-iran-hackers-exclusive-idUSKBN1ZZ1MS .

Taylor, R. (2015). The need for a paradigm shift toward cybersecurity in journalism. National Cybersecurity Institute Journal, 1(3), 45.47–

Thorsen, E. (2019). Surveillance of journalists/encryption issues. In T. Vos & F. Hanush (Eds.), The international encyclopedia of journalism studies. Wiley.

Tsui, L. (2019). The importance of digital security to securing press freedom. Journalism, 20(1), 80.82–

Tsui, L., & Lee, F. (2019). How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. Journalism. https://journals.sagepub.com/doi/pdf/10.1177/1464884919849418 .

Wahl-Jorgensen, K., Bennet, L. K., & Jonathan Cable, J. (2017). Surveillance normalization and critique: News coverage and journalists 'discourses around the Snowden revelations. Digital Journalism, 5(3), 386.403–

Wahl-Jorgensen, K., Williams, A., Sambrook, R., Harris, J., Garcia-Blanco, I., Dencik, L., Cushion, S., Carter, C., & Allan, S. (2016). The future of journalism: Risks, threats and opportunities. Digital Journalism, 4(7), 809.815–

Waters, S. (2018). The effects of mass surveillance on journalists 'relations with confidential sources. Digital Journalism, 6(10), 1294.1313–

Wootliff, R. (2016, April 6). Israelis arrested for spying on Romanian anti-corruption czar. The Times of Israel.