ephemera
theory & politics in organization

ISSN 1473-2866 (Online)
ISSN 2052-1499 (Print)
www.ephemerajournal.org
volume 19(4): 807-824

How to protect the truth? Challenges of cybersecurity, investigative journalism and whistleblowing in times of surveillance capitalism. An interview with Micah Lee

Micah Lee and Randi Heinrichs

abstract

We are witnessing a crisis of information security. Massive data monitoring is both a condition and an expression of this crisis. Connected whistleblowing cases like the Snowden leaks deal with both – they result from these conditions, act against them and have to consider them during the process of revelation. Whistleblowers therefore need expertise in cybersecurity, just as investigative journalists do. However, the interview makes the point that this is not just a technological issue. The 'problematization' of truth-telling in digital cultures is much more complex. It is connected to large-scale transformations of highly digitized societies under the conditions of surveillance capitalism. The following contribution presents an interview with the investigative journalist, cybersecurity specialist and privacy activist Micah Lee, and discusses the challenges of truth-telling in a powerful global surveillance apparatus and the crisis of information security.

Introduction

Micah Lee is a technical specialist in operational security, source protection, privacy, and cryptography. He is also a founding and board member of the Freedom of the Press Foundation[1] and a journalist at the investigative news

1 https://freedom.press.

organization The Intercept[2]. Regarding his commitment to the Snowden revelations, Mashable Spotlight (Franceschi-Bicchierai, 2014) called him the 'digital bodyguard' of the NSA leaks.

Before Edward Snowden became a whistleblower in 2013, he contacted Micah Lee for help. Snowden had to face a big challenge: how could he get in contact with the journalists Glenn Greenwald and Laura Poitras anonymously and securely? Of course, Snowden himself is an expert on cybersecurity, but to protect the information and his own anonymity until the moment of publication he had to rely on the cooperation of the receivers' side, too. As he had served the CIA (Central Intelligence Agency), NSA (National Security Agency), and DIA (Defence Intelligence Agency) for nearly a decade, he knew how complicated the process of leaking information about the NSA's wide-ranging surveillance system without being caught in the middle of it would become. To plan a secret meeting in Hong Kong and to hand over the information classified as top secret to the journalists, they would have to install and use an encryption program like *Pretty Good Privacy* (PGP)[3]. Snowden needed the help of an expert who would build up a secure communication infrastructure, would understand the importance of the political mission, and who was willing to take a immense personal risk with his engagement against state surveillance.

Micah Lee was the perfect match. It is still rare to find someone who fits all these qualifications, even though far-sighted expertise is highly needed in times of networked news organisations, and connected challenges for information security, and therefore for journalism more broadly (Stalder, 2010). With the help of Micah Lee and the involved journalists, Edward Snowden revealed that the NSA was unconstitutionally collecting the data records of billions of individuals who had not been suspected of any wrongdoing or of terroristic or criminal activity. To understand the surveillance apparatus in depth, critical questioning of the government's security policy and a swelling data economy had to be combined with technological expertise of the software they used.

Computer-enabled data collection, aggregation, and mining dramatically change the nature of contemporary surveillance, but what the NSA leaks also showed is how the booming „international surveillance technology industry" (Verde Garrido, 2015: 157) is based on the extensive cooperation of governmental institutions and private tech companies. The program *PRISM* (Planning Tool for Resource Integration, Synchronisation and Management) had collected and continuously analysed server data from companies like AOL, Apple, Google,

2 https://theintercept.com

3 https://www.openpgp.org

Facebook, Microsoft, PalTalk, Skype, Yahoo and Youtube. We witness an increasing neoliberalization of state functions, especially those concerned with security, that are cooperating closely with industries that commercialize the monitoring, collection, and processing of vast amounts of information about people all over the world (*ibid.*). According Amnesty International's estimates (2014) the total turnover behind the surveillance industry during the Snowden revelations was between three and five billion US dollars, and it is growing by 20 per cent every year. This is not limited to the US context. The leaks about the operation *Tempora* showed how the Five Eyes consisting of the NSA, the British GHCQ (Government Communications Headquarters) and their partner institutions from Canada, Australia and New Zealand monitored immense volumes of electronically transmitted communication. The Snowden revelations proved that all Western industrial nations profit from the Five Eyes countries' cooperation (Greenwald, 2014). The declared reason behind investigative user surveillance from the state institutions was and still is that with the help of the monitoring systems, terrorism suspects can be recognized early on and potential attacks could be prevented. Its legitimatizing excuse to protect national security was used to justify the collection of huge amounts of metadata about who was where and when, connected with whom and for how long (Sprenger, 2015). This massive data gathering in the name of alleged security becomes a technique of governmental power as well as a lucrative business model (Lyon, 2002). That Snowden leaked information about the global surveillance system, and that cryptography and privacy-enhancing technologies are used to obfuscate data monitoring are seen as dangerous disruptions of the powerful security apparatus. The leaks resulted in the largest debate about reforms to US surveillance policy and global monitoring practices, including questions around current conditions for a free press (Bauman et. al., 2014; Greenwald, 2014; Lyon, 2014).

After writing about the massive surveillance while being continuously under the fear of exposure Micah Lee, Glenn Greenwald, Laura Poitras, and Jeremy Scahill started a news organization called The Intercept. The Intercept supports software like SecureDro[4], which is a whistleblowing submission tool that allows news organizations to accept documents from anonymous sources.

In this interview Micah Lee tells the story of his involvement in the NSA whistleblowing case of Edward Snowden and why it is increasingly important to think about the role of cybersecurity, anonymity and open software in processes of revealing the truth, whistleblowing and investigative journalism in the 'age of surveillance capitalism' (Zuboff, 2019). In the context of this special issue the interview raises questions of what consequences, challenges and new

4 https://securedrop.org

opportunities there are for specific connectivity in a digital age, and what they provide for the conditions of 'truth-telling' (Foucault, 2001). The following interview was held on the 9th of July 2018 in Berkeley, CA, USA.

The interview

Randi Heinrichs:

When you first got involved with the NSA revelations you were working at a digital rights organization, the 'Electronic Frontier Foundation' (EFF)[5]. How did you get involved with digital activism and the fight for privacy and free speech?

Micah Lee:

Before I got my job at EFF I was working as a web developer for a long time, but I had been interested in encryption and topics around online freedom, etc. before. I was always fascinated by it. For the first time I really got deeply involved in digital security questions at EFF. Therefore I was incredibly excited to be hired by them. When I started working at EFF I also did web development at first and eventually I became a staff technologist there. So, I came from software development and was also doing lots of web activism.

RH:

Besides being a web developer, you are also one of the founders and board members of the Freedom of the Press Foundation and you work as a journalist at The Intercept, a news organization that covers topics like national security, civil liberties, international affairs, technology and criminal justice. Why do computer engineering and especially computer security have an increasingly important role for journalism and whistleblowing?

ML:

It used to be that you as a journalist could protect your sources. If you wanted to protect an identity from any sort of investigations, you could go, for example, to a payphone and make a call to meet and talk in person. It used to be that if you really needed to protect your source, you could just not tell the government who your source was and that worked pretty well. Things have completely changed now; everything is being spied on. Now the government can just look through your e-mails or through your text messages or through all of the digital evidence

5 https://www.eff.org

that exists. In most situations you will need to use phones, you will need to use computers, you will need to use the Internet – and it's really difficult to do it without leaving lots of traces everywhere. So, I think that's why computer security is very important in journalism.

RH:

To have a secure connection between the journalists and the source or the journalist and the whistleblower is becoming increasingly difficult. Computer security engineers have an important position as a protecting middleman. This brings, of course, a lot of responsibility to new players involved. What are the biggest challenges to those in that position?

ML:

Well, there are a lot of challenges. One of them is source protection. Nowadays the news organizations are getting a lot more digital security training, and therefore understanding of how to use encryption – a lot more than the actual sources. The journalists are only one side to protect the communication with the source. A good first step is to set up something like SecureDrop, which makes it hard for sources to make mistakes. Even though a lot of times the source might get in contact with a news organization by using SecureDrop and when they have another question they just send an e-mail, which leaves lots of records. If you're using for example Gmail, leak investigators could subpoena the mail. Ultimately the journalists only have control over ten or fifteen percent of protecting the source. I think that's the biggest challenge.

RH:

Mashable Spotlight called you the 'digital bodyguard' of the NSA leaks. How did you get in contact with Snowden and the journalists Laura Poitras and Glenn Greenwald who then worked on the NSA revelations?

ML:

This was the end of 2012 and the beginning of 2013. The Freedom of the Press Foundation was just was founded by Trevor Timm. He is the Executive Director now, but at the time he was working with me at EFF. I was still working full time at EFF and helped him part time as the CTO of the Freedom of the Press Foundation. That means I built the website and I did all of the technical stuff to start it. Glenn Greenwald and Laura Poitras and a bunch of other people were with me on the board of directors of the Freedom of the Press Foundation. About a month after the website was launched, I got an encrypted e-mail from an

anonymous person. This turned out to be Snowden. The reason why he wrote to me, was to get in contact with Glenn Greenwald and Laura Poitras. At the time Snowden had already tried to contact Glenn, but he didn't actually tell him anything, because Glenn wasn't using encryption yet. Snowden had sent him some instructions on how to use encrypted e-mail. Glenn didn't take the time to do it. It is to say, that it was much harder to use encryption back than. I think that this is one of the big things that have changed over the last six years. Encryption is much more usable and people are realizing that. Usability is a really important security feature. If you don't know how to use encryption, then you aren't going to use it.

RH:

There was a rumour that because Glenn Greenwald did not use encryption for his e-mails the NSA leaks were postponed for more than half a year.

ML:

Yeah. I think they were. Snowden also wanted to talk to Laura Poitras. He knew that she was already using PGP and it would therefore be much easier to have a secure conversation with her, but he didn't know what her PGP fingerprint[6] was. When he went to the Freedom of the Press Foundation website, he saw that I was the only person that had a PGP fingerprint listed online in my bio. So, he anonymously sent me an encrypted e-mail. I didn't know who he was. He was just saying: 'I am a friend. Could you help me talk to Laura Poitras? Can you give me her PGP key? I promise it is for something good, and while you're at it can you help teach Glenn Greenwald how to use encryption?'

RH:

You ended up publishing Laura Poitras' PGP fingerprint on Twitter. It feels counterintuitive to use a public online platform like Twitter for communicating while you are trying to keep a secret.

ML:

Snowden was concerned that he wasn't having this conversation with *me*. We didn't talk in person. Our only communication was with these PGP encrypted messages. What if my computer was hacked or something went wrong? He downloaded my PGP key from our website, but what if he was intercepted, his download was intercepted or he was encrypting with the wrong key and he was

6 https://en.wikipedia.org/wiki/Public_key_fingerprint

actually talking to someone who works for the government and not with me? Using Twitter is a way of confirming that the Micah Lee that was controlling the e-mail is the same Micah Lee that controls the Twitter account. If my e-mail account was hacked and there was some sort of 'PGP-man-in-the-middle-attack'[7] going on, they would have to do a lot more to also compromise my Twitter account in real time. Basically, we were using multiple channels to verify that he was talking to the correct person.

RH:

It's interesting that you had to verify your identity on multiple channels while he was still anonymous and to prove that it could stay this way. Why did you trust him?

ML:

Yeah. I just did. I mean nobody knew at the time. I didn't know who he was. He was just a stranger. It took me probably several months of talking to him, and to Glenn and to Laura before I got the sense that he was a whistleblower. Even then I had no idea about what he was blowing the whistle on.

RH:

Today we know who was behind the NSA leak. Snowden became a public and symbolic figure in the debate around Internet freedom, privacy and surveillance in the digital age. Why do you think he decided not to stay anonymous?

ML:

Well, I think that the real reason why he made that decision is because he realised that there is no way he would have been able to keep his identity a secret – especially with the amount of stuff that he was leaking. The NSA is incredibly powerful and nobody knew that better than him. He knew that it would be too hard to keep it a secret for a long time and he wanted to be upfront and open about why he did it. So, in the end, he made a decision that he wasn't even trying to hide his tracks.

7 https://www.thesecuritybuddy.com/vulnerabilities/what-is-man-in-the-middle-attack/

RH:

It was a dangerous and risky endeavour for everyone involved. I read that you have been very concerned that someone could identify you with your personal style of coding.

ML:

Yeah. I hadn't actually considered it until I was trying to anonymously develop a website. We ended up in situations in which Snowden even had to pay for the webhosting in his own name with his own credit card and stuff like that … I didn't want my involvement to be public until I would decide that it was safe to be public. Part of that involved protecting my anonymity as a programmer. I was using the anonymous browser Tor[8] to connect to the server and pushing[9] the website code to the server etc.. So, I was writing it anonymously, but you can view the source of a website, you can see the design and the style. Everything was very consistent with the style in which I have always done my stuff. So, I was worried that my coding style could give me away.

RH:

For most of the leaking process you used open-source-software like Tor, PGP, OTR[10]. Why? Does the involvement of a whole community behind the open-software projects make these programs more transparent and more secure or is the contrary the case?

ML:

I think that there are a couple of things to consider. For security software and very secure critical software it is really important to be able to trust that the software does what it says it does. When you publish your source code, like open-software projects do, it allows experts to look at it, to audit it, and to make sure it does what it says it does. However, that's not to say that it's necessarily more secure. There are a lot of really insecure open source programs. For example, the Linux Kernel[11] is full of bugs, but making it open gives you a lot of transparency on how it works. This gives also a lot more faith that the software is not actually malicious, that it doesn't have some sort of backdoor. There is proprietary

8 https://www.torproject.org

9 https://www.techopedia.com/definition/5732/push-technology

10 https://www.otr.im/chat.html

11 https://en.wikipedia.org/wiki/Linux_kernel

software like Skype that advertised itself for a very long time as end-to-end encrypted, but it had a backdoor for the US government. There was no way to verify this. Snowden was especially aware of this problem because he knew that the NSA actively worked to get backdoors in proprietary software. If you work for the NSA and you're going to try to get a backdoor into proprietary software, you just need to make the right friends at the company. You tell them it is all for national security and hopefully you find people that agree on the mission and are willing to work with you. If on the other hand you try to get the same backdoors into an open-software project, you need to go through an open process, where all of the source code is open, and every single commit[12] is open. Therefore you would have to pretend that you are going to add a new feature. When they merge your feature it secretly would have a bug that only you know about, or something like that. It's much more complicated to do that.

RH:

Some people argue that we are living in a time of the end of anonymity and that this hasn't changed after the Snowden leaks. What do you think about that?

ML:

I don't think that is true. It's so much easier to use encryption now then it was in 2013. It used to be that you had to learn how to use an encryption tool like PGP. You'd have to understand something like key management and key pairs and verifying fingerprints and all that stuff. Now you can just install a program like Signal[13] and use it to send an encrypted message to somebody. There are still some things that you should understand, like verifying the safety numbers[14] in Signal to make sure there isn't an attack going on, but it's much simpler. This is one of the main things that the Snowden leaks changed. It prompted a lot of people to improve the technology and fix some of the security holes that had been getting exploited for a really long time. I also don't think that there is ever going to be the end of anonymity as long as there's not literal fascism everywhere – well, we'll see how that goes. There are always people thinking and working on anonymity and coming up with new ideas.

12 https://en.wikipedia.org/wiki/Commit_%28version_control%29

13 https://signal.org

14 https://support.signal.org/hc/en-us/articles/360007060632

RH:

Snowden was highly influenced by other whistleblowers who took the risk of truth telling before him, like the first person publicly called a whistleblower, Daniel Ellsberg, who leaked the Pentagon Papers about the decision-making of the US government in the Vietnam War in 1971; or Chelsea Manning, the former United States Army soldier who disclosed nearly 750,000 military and diplomatic documents that came to be known as the Iraq War Logs and the Afghan War Diary in 2010. If you compare the case of Chelsea Manning, who copied thousands of intelligence files on a CD, labelled it with the singer's name *Lady Gaga* and sent it to WikiLeaks to the case of Daniel Ellsberg, who copied over a period of two years 47 paper files by hand in the Pentagon, it illustrates that the digital networked infrastructure makes it easier to get and move the information.

ML:

It makes it much easier that you don't have to use copy machines and that you can use the Internet. What Daniel Ellsberg likes to say is that before he photocopied the Pentagon Papers, he had planned to blow the whistle about the entire history of the US nuclear program. The Pentagon Papers were actually the smaller leaks. He just felt like the Pentagon Papers were more pressing. He ended up hiding the other papers in a box at his brother-in-law's house. His brother-in-law buried them somewhere, waiting for him to get out of prison. When he got out of prison he would leak all of the rest of the nuclear secrets for preventing a nuclear holocaust – but then there was a hurricane that destroyed them. That's the reason why we didn't get this leak later. Daniel Ellsberg likes to say: He was in the military, he served in Vietnam and he was totally willing to die for his country, when he realized how much of a fraud the Vietnam War was and also how incredibly close to the end of humanity the world has come several times. He was just as willing to die for preventing the world from having a nuclear Holocaust and stopping the Vietnam War. I think that his whole risk assessment was: 'yeah, this is a huge risk to photocopy all of this papers and drive around the country dropping it off with journalists or whatever, but it's worth it,' – even if he got caught. The technology makes it much easier to do whistleblowing, but it also makes it much easier to catch people. Daniel Ellsberg, Chelsea Manning, Edward Snowden, and a few other people all got caught, right? I think there's a lot of leaks where whoever leaked them is still anonymous, but there's a lot of them where people got caught. The ubiquitous surveillance makes it really hard to do this without getting caught. You have to kind of be an expert.

RH:

One open question is, did these whistleblower even try not to get caught? Snowden for example wasn't actually caught. One could say regarding the fact that there had been NSA whistleblowers before Snowden, that especially the risk he was willing to take publicly made his story reliable. The fact that he is still in Moscow and that he sacrificed the life he used to live make what he did trustworthy and even more momentous – and therefore maybe more powerful.

ML:

Right. Snowden clearly didn't try not to get caught. Chelsea Manning was trying to remain anonymous, like Daniel Ellsberg did. I think that when you're a whistleblower there is just so much stacked against you. It's an enormous risk that you are taking, because you feel it's so incredibly important. I think that everybody who is blowing the whistle on something that big can't do it without also facing also a big risk. There's some sort of sacrifice. You know that you might get caught.

RH:

Well, it seems there is always also a very personal background involved in these whistleblowing cases. Interestingly the most well-known whistleblower of our time seem to be connected to their expert knowledge about technology or even surveillance technology, right? So, it seems the battlefield switched.

ML:

Yeah, well, I mean, I think the battlefield for everything has switched to technology, and the Internet.

RH:

Is this the reason why you spent a lot of time teaching people how to secure their communication? Why do you think it's so important to teach encryption to the broader public? Do you think about encryption also as a form of resistance against the government surveillance or even as a form of critique?

ML:

I did a lot of encryption training explaining how encryption works to people and stuff while I was working at EFF. I helped to write parts of the Surveillance Self

Defense Guide[15] which EFF hosts, which is a series of tutorials for all sorts of mostly encrypted communications, encrypting your hard drive or things like that. I did this also for a broader public, but mostly for activist communities and journalists. Even after the Snowden leaks a lot of people don't realize the extent to which they lost the ability to preserve their privacy. It used to be much more challenging to eavesdrop on a phone call. The phone company could tap a specific phone line, but they didn't have the capability to tap all of the phone lines. You had to be a suspect for your phone call to be listened to and there had to be an investigation. Someone had to go to your house and install a tap into the phone line that went into your building. Now it is just trivial to tap everybody and record it forever. I think that people don't realize that there used to be this level of privacy that with advanced technology everybody lost. Encryption is just a way to bring some of it back. That's why it is important for everybody.

RH:

To raise awareness about these issues, you worked with Snowden on a website to publish a manifesto against surveillance. Why did you decide not to publish it?

ML:

The website was a contingency plan that didn't need to happen. Snowden was concerned that he would try to blow the whistle and it wouldn't work. He was concerned that the Guardian wouldn't publish it and the US, the UK and the rest of the Five Eyes intelligence agencies would successfully squash the story. All of the documents would get seized from the journalists and he would just be in solitary confinement and he wouldn't have any voice. If all of that were to happen, he would still have a voice with the manifesto online even though he would be in prison, not allowed to talk to anybody. He was worried that what happened to Chelsea Manning would happen to him. That didn't end up happening, and so we didn't end up publishing it.

RH:

What are you working on right now?

ML:

I'm still working at The Intercept. I'm doing a lot of journalism. One thing that I've been spending a lot of time with at The Intercept is publishing the rest of the material from Snowden. We're the only news organization that has the Snowden

15 https://ssd.eff.org/en

archive and is still publishing from it. One section of the Snowden archive is called SIDtoday[16]. We've been systematically publishing from it for a couple of years now. SIDtoday was an internal newsletter, like an internal blog, that anyone who is part of the Five Eyes could read. It was The Signal's Intelligence Director at NSA who ran it. It is all classified information. We've been going through the blog and are publishing every single post of it. We published everything from 2003, 2004, 2005 – we are finishing up 2006 and getting to 2007. There is still really fascinating stuff in there even though most of it is kind of administrative. I've been spending a lot of time on going through the material with a team of people reading every single document, writing a summary of it and categorizing which ones are the most interesting ones and which ones aren't. Then we are writing articles about it and publishing them all in bulk. We published a few thousand documents so far.

RH:

Wow, that sounds like a lot of very detailed, specialised and time consuming work. Why are the documents of the SIDtoday especially important?

ML:

Well, one thing about the material from SIDtoday is, that unlike almost everything else in the archive of the Snowden documents, this is human readable. It is actually designed and written for a general audience including people who have a lot of technical skills as well as people who don't. It is giving status updates and describing their cool new programs that they are launching and things like that. The rest of the archive is really hard to understand. All of the programs have code words or it is a very technical thing and a lot of times there is not even enough context to really understand what a program is doing or what something is about. There is a lot of missing information, but SIDtoday is very accessible. I think that it's important because more than anything else, with these materials we can start to make public the secret history of what the United States did since the beginning of the War on Terror.

16 In the meantime The Intercept concluded the analysis of material stemming from the SIDtoday in May 2019. They published more than 2,000 NSA documents over the time of four years. See: https://theIntercept.com/snowden-sidtoday/

RH:

Thank you very much for your hard and very important work. For me this whole stretch of history is still pretty much unbelievable.

ML:

For me, too.

Concluding thoughts

Micah Lee and I met for the interview at *The Musical Offering*, one of the last existing CD shops in Berkeley, California. Across the San Francisco Bay and Silicon Valley, the centre of the world's most powerful tech and social media companies, the small Café is filled with a nostalgic atmosphere accommodating tons of CDs, and students scribbling in paper notebooks next to the Campus of the University of California, Berkeley. UC Berkeley is the university where Michel Foucault gave his lecture series *Discourse and Truth: the Problematization of Parrhesia* in 1983, which constitutes an important theoretical background for this special ephemera issue. Towards the end of the lectures Foucault (2001: 169) explains that his 'intention was not to deal with the problem of truth, but with the problem of the truth-teller or truth-telling as an activity.'

The interview offers important insights to the conditions of truth-telling as well as to the 'problematisation' (*ibid.*: 171) of the truth-teller and the act of truth-telling in the context of the contemporary mass-mediated knowledge economy. In our present time truth-telling is mediated in multiple ways: by the ubiquity of digital media, by institutional, technical and social regulations, and in the specific case of whistleblowing by intermediary organisations that seek to support, channel or capitalise truth-telling in the name of more transparency, democracy or justice. With the consideration of a multi-layered mediated truth-telling process the interview points out specific opportunities and challenges in relation to power, resistance and critique in contemporary surveillance societies (Di Salvo, 2016; Olesen, 2019).

Generally speaking the very fact that the classified NSA documents could be leaked in the first place, shows that disruptive practices against global surveillance systems are (still) possible, and in certain sense are even facilitated by digital media infrastructures. Before Daniel Ellsberg became the first publicly known whistleblower in 1971, he secretly photocopied paper documents, later known as the Pentagon Papers, over a period of almost two years. In his memoirs he describes the painstaking process: 'One hand picked up a page, the

other fit it on the glass, top down, push the button, wait ... lift, move the original to the right while picking another page form the pile ...' (Ellsberg, 2003: 302). He smuggled 47 volumes out of the Pentagon building and handed them over to the journalists of the New York Times and later the Washington Post (*ibid.*). The possibility to copy and paste documents on a digital hard drive or upload them on a networked computer has fundamentally changed the conditions of the overall act (Stalder, 2010).

However, the reasons for secret services' tremendous difficulties in protecting classified state documents are more complex than the change of this information's materiality from analogue to digital. While Ellsberg was contributing to the top-secret study of classified documents as a high-level United States military analyst, and therefore had physical access to the archive within the government building, the 29-year-old Edward Snowden had access to the NSA-Intranet *NSAnet* as one of over 1000 Sysadmins working for private defence and intelligence consulting firms like Booz Allen Hamilton (Harding, 2014). The on-going outsourcing of intelligence work and cooperation of state institutions with external contractors heightens the need for classified records to be accessible and moveable within a larger network of allies. 'This creates the techno-organisational preconditions for massive amounts of information to leak out,' as Felix Stalder (2010) puts it in a nutshell. The media-technological conditions that enable the secret services' surveillance practices and those of cooperating industry organizations, also offer the possibilities for disruptive acts like leaking. It is still not publicly known how Snowden moved the documents from the NSA system, but it seems quite obvious that the operative level of whistleblowing becomes easier with digital media – even though the relevant technical and organisational considerations Lee explains within this interview also demonstrate the emergence of new complexities. The central role of Lee's expertise for the revelations as a journalist, as a technical cybersecurity specialist, as a programmer of the manifesto-website, and as a privacy activist, indicates specific requirements for the act of truth-telling under the conditions of networked information infrastructures and the hegemony of a global surveillance apparatus. It might be easier to get and leak information, but it is also easier to get caught while doing it. The crisis of information security affects the overall process of truth-telling. Therefore new expertise for the act of truth-telling is needed and new players are rising. Investigative journalists, especially those reporting on government and national security, just like whistleblowers, are depending on special knowledge on cybersecurity.

The fact that Micah Lee was contacted by Edward Snowden, because he was the only one who offered an encryption key on the website of the Freedom of the Press Foundation as well as the fact that Glenn Greenwald wasn't able to use the

program PGP and therefore postponed the publication for six months are vividly demonstrating, how challenging and crucial the protection of source and information have become for whistleblowing and a functioning press. Information security is an issue of press freedom and more broadly for truth-telling in general. In this context Micah Lee's work at a news organisation like The Intercept, just as the work of NGOs like the Electronic Frontier Foundation and their security trainings for journalists and activists appear as a critique against the practices of massive monitoring of communication. Their engagement becomes a form of truth-telling about information-governance within the global surveillance apparatus itself.

It seems that it is not the extent of what the journalist Glenn Greenwald (2014: 8) calls the 'secret systems of suspicionless surveillance' that has changed after the NSA leaks, but the accomplishments in the field of privacy enhancing software, which stand against it. New services like the open source whistleblower submission system *SecureDrop* are much easier to use. They are now available and help to protect the truth-teller and his or her information. But the interview also highlights that it takes more than a technical solution to face complex new challenges. Open software might not be more secure in a technical sense, but the transparent source code and the principle of *many eyes* from the open software community can make the services trustworthy. This also demonstrates that transparency and secrecy are not opposites in digital cultures – they can support one another. Open software or the use of a public online platform like Twitter can be of help to keep a secret and protect other people's anonymity.

It is important to take into account that the new challenges in the truth-telling process are deeply entangled with large-scale transformations of digital cultures. In the context of 'surveillance capitalism' (Zuboff, 2019) the extraction and monitoring of masses of data is both a condition for and an expression of a new logic of accumulation. Recent whistleblowing cases are shaped by these conditions: they act with them and against them – and they have to be considered in the process of making the 'truth' seen, heard and recognised by a wider public. Whistleblowers and journalists who are addressing the issues regarding the powerful global surveillance apparatus and make the crisis of information security visible are increasingly scorned or criminalised as 'traitorous violators' of national security, hackers, spies and dangerous betrayers of secrets (Scheuerman, 2014).

Therefore it seems urgent to end the discussion of this interview with a rather political statement: that the disclosure of classified state information via leaking is suddenly a signature of our time seems not to demonstrate a criminal destructiveness of single dissidents. Instead, it seems to be a sign of disruption

within the security apparatus structured by the economic rules of surveillance capitalism (Bazzichelli, 2014). Journalists like Micah Lee and whistleblowers like Edward Snowden make this disruption visible; they are not the reason for the disruption.

references

Amnesty International (2014) Coalition against unlawful surveillance exports (cause). q&a of 4th of April 2014 [https://www.amnesty.org/en/latest/news/2014/04/questions-and-answers-coalition-against-unlawful-surveillance-exports-cause/].

Bauman, Z., D. Bigo, P. Esteves, E. Guild and V. Jabri (2014) 'After Snowden: rethinking the impact of surveillance.' *International Political Sociology,* (8): 121-144.

Bazzichelli, T. (2014) 'the disruptors!' *exberliner*, 4th November [http://www.exberliner.com/features/lifestyle/the-disruptors/].

Di Salvo, P. (2016) 'Strategies of circulation restriction in whistleblowing. The pentagon papers, WikiLeaks and Snowden cases.' *TECNOSCIENZA: Italian Journal of Science and Technology Studies,* 7(1): 67-85.

Ellsberg, D. (2003) *Secrets: A Memoir of Vietnam and the Pentagon Papers*. London: Penguin Books.

Foucault, M. (2001) *Fearless speech*. Los Angeles: Semiotext(e).

Franceschi-Bicchierai, L. (2014) 'Meet the man hired to make sure the Snowden docs aren't hacked.' *Mashable Spotlight*, 27th May [https://mashable.com/2014/05/27/micah-lee-greenwald-snowden/?europe=true#jDEylFrFlZqd].

Greenwald, G. (2014) *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Metropolitan Books.

Harding, L. (2014) *The Snowden Files: The Inside Story of the World's Most Wanted Man*. London: Guardian Faber Publishing.

Lyon, D. (2002) *Surveillance society: monitoring everyday life*. Buckingham: Open University Press.

Lyon, D. (2014) 'Surveillance, Snowden, and big data: capacities, consequences, critique.' *Big Data and Society,* July-December: 1-13.

Olesen, T. (2019) 'The politics of whistleblowing in digitalized societies.' *Politics and Society, 47*(2): 277-297.

Scheuerman, W. E. (2014) 'Whistleblowing as civil disobedience.' *Philosophy and Social Criticism,* 40(7): 609-628.

Sprenger, F. (2015) *Politics of micro-decisions. Edward Snowden, netneutrality and the architectures of the internet*. Meson Press [https://meson.press/wp-content/uploads/2015/04/9783957960412-Sprenger-The_Politics_of_Micro-Descisions.pdf].

Stalder, F. (2010) 'Contain this! Leaks, whistleblowers and the networked news ecology.' *Eurozine* [https://www.eurozine.com/contain-this/].

Verde Garrido, M. (2015) 'Contesting a biopolitics of information and communications: the importance of truth and sousveillance after Snowden.' *Surveillance & Society,* 5(2): 153-167 [http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/snowden_biopolitics].

Zuboff, S. (2019) *The age of surveillance capitalism*. New York: Public Affairs.

the authors

Micah Lee is *First Look Media's* Director of Information Security. He is a computer security engineer and an open-source software developer who writes about technical topics like digital and operational security, encryption tools, whistleblowing, and hacking. He develops security and privacy tools such as *OnionShare* and *semiphemeral*.
Email: micah.lee@theintercept.com

Randi Heinrichs is a PhD candidate at the Leuphana University, Luneburg, where she is working on her dissertation on anonymity, social media platforms and (data-) neighbourhoods. Her research interests, teaching, and writing are located at the intersections of digital cultures, technology, and questions around anonymity, agency, and discrimination. She is a member of the editorial board of the journal *spheres* and a collective member of *ephemera*.
Email: randi.heinrichs@leuphana.de