Analysis

A world without wiretapping? Official documents highlight concern over effects 5G technology will have on "lawful interception"

Chris Jones

June 2019

The introduction of 5G telecommunications networks could render traditional "lawful interception" techniques used by the police obsolete, according to internal EU documents. Discussions on how to deal with the issue are ongoing – but are being kept behind closed doors. There is a need for a public discussion on this issue, as well as the closely-related topic of the surveillance potential of new technologies facilitated by 5G that threaten to introduce – in the words of a police think tank, no less – "major invasions of privacy and a fundamental, and at this stage unregulated, shift in the relationship between the police and the public."

Contents

1. Introduction 2
2. Trouble for lawful interception 2
   2.1. Identifying and locating individuals and their devices 3
   2.2. Availability and accessibility of information 4
      2.2.1. A piece of cake 4
      2.2.2. Close to the edge 4
      2.2.3. End-to-end encryption 5
      2.2.4. A security problem: network function virtualisation 6
3. What is to be done: the law enforcement view 6
   3.1. Setting standards 6
   3.2. New laws 7
   3.3. Police working groups 8
4. Out with the old, in with the new 9
5. The need for public debate 11

1. Introduction

The spectre of Chinese technology company Huawei controlling the 5G telecommunications infrastructure currently being installed across western states has recently become a major media and political issue.[1] However, 5G is also causing panic amongst European security officials, for an entirely different reason – the new technology may dramatically undermine the ability of law enforcement agencies to carry out "lawful interception" (more commonly known as wiretapping) of telecommunications.

Proposals for dealing with the situation include influencing the work of international standard-setting bodies and introducing new legislation to enforce technological requirements upon telecoms companies. This could be necessary, according to Europol and the EU's Counter-Terrorism Coordinator, to ensure that wiretapping remains possible. On the other hand, given that 5G is supposed to provide the backbone of the 'Internet of Things', vast new troves of data are likely to become available to law enforcement agencies, whether or not existing lawful interception practices remain possible. So far, the only debate on this issue has taken place behind closed doors – but given the implications for civil liberties, a much more public discussion needs to take place.

2. Trouble for lawful interception

It seems that amongst the states of the 'Five Eyes' spying alliance (Australia, Canada, New Zealand, the UK and the USA), the issues raised by 5G technology for law enforcement agencies have only been raised publicly in Australia. In February 2018, the country's interior ministry and law enforcement agencies made a submission to a parliamentary inquiry arguing that "5G and IPv6 technologies will make it significantly more difficult to access communications," warning that "this could result in an 'exponential burden' for telcos [telecoms companies] and government."[2]

Now the debate is coming to the EU, although at the moment it is only taking place behind closed doors. Gilles de Kerchove, the EU's Counter-Terrorism Coordinator, sent a briefing document to EU member states' delegations in the Council of the EU at the beginning of May. He put it plainly:

> *"5G will make it harder for law enforcement and judicial authorities to carry out lawful interception. Due to 5G's high security standards and a fragmented and virtualised architecture, law enforcement and judicial authorities may lose access to valuable data."*[3]

---

[1] 'Huawei: Which countries are blocking its 5G technology?', *BBC News*, 18 May 2019, https://www.bbc.co.uk/news/world-48309132

[2] Allie Coyne, 'Aussie law enforcement warns telcos of 5G, IPv6 data access 'burden'', *itnews*, 26 February 2018, https://www.itnews.com.au/news/aussie-law-enforcement-warns-telcos-of-5g-ipv6-data-access-burden-485897; Australian Government Department of Home Affairs, 'Joint Submission to the Inquiry into the Impact of New and Emerging Information and Communications Technology', http://www.statewatch.org/news/2019/jun/aus-interior-ministry-submission-new-technologies-2-18.pdf

[3] 'Law enforcement and judicial aspects related to 5G', Council document 8983/19, LIMITE, 6 May 2019, http://statewatch.org/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf

Further detail on the technical issues is provided in a document produced by Europol and sent to the Council's Law Enforcement Working Party (LEWP) in mid-April.[4] These come under two main headings: "identification and localisation of users" and "availability and accessibility of information".

2.1. Identifying and locating individuals and their devices

Currently, it is possible to identify every single mobile phone individually through the IMSI (International Mobile Subscriber Identity), a unique code attached to the device "which is sent in the background during every communication process and which can be used to identify and locate the mobile phone device," in the words of the Europol document. The plan for 5G networks and devices, however, is to encrypt the IMSI, meaning "the security authorities are no longer able to locate or identify the mobile device," and will be "unable to assign a device to a specific person" through requests to telecommunications companies for user data.

At the same time, 5G could make IMSI catchers obsolete. Also known as "stingrays" in the US and Canada, IMSI catchers have been described by *Privacy International* in the following way:

> *"An IMSI catcher is an intrusive piece of technology that can be used to locate and track all mobile phones that are switched on in a certain area.*
>
> *An IMSI catcher does this by 'pretending' to be a mobile phone tower - tricking your phone into connecting to the IMSI-catcher, and then revealing your personal details without your knowledge."*[5]

The ability to access information on IMSI codes is extremely useful to police forces, because the code is attached to an individual mobile device, rather than to a SIM card, which can be more cheaply and easily changed than the device itself. *Privacy International* argue that IMSI catchers are "indiscriminate surveillance tools that could be used to track who attends a political demonstration or a public event like a football match." Europol's paper describes them, on the other hand, as "one of the most important tactical operational and investigation tools" and "indispensable for carrying out lawful surveillance of persons who frequently change their Subscriber Identification Module (SIM)."

Love them or hate them, 5G looks set to make IMSI catchers extinct. 5G will employ something called "false-base detection," a new function "that enables both the mobile network of providers and the mobile devices of the users to detect 'false' base stations such as the IMSI catcher." As a result, warns the policing agency, "there is the danger that it would no longer be possible to carry out legally permissible, technical investigation and surveillance measures."

---

[4] 'Position paper on 5G by Europol', Council document 8268/19, LIMITE, 11 April 2019, http://statewatch.org/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf

[5] 'IMSI Catchers', *Privacy International*, https://www.privacyinternational.org/explainer/2222/imsi-catchers

2.2. Availability and accessibility of information

Three separate issues are raised by Europol under this heading: "network slicing"; "Multi-Access Edge Computing (MEC)"; and one of the old nemeses of law enforcement and security agencies, end-to-end encryption.

2.2.1. A piece of cake

Network slicing makes it possible to set up numerous digital networks, performing different functions and activities, on the same physical infrastructure. The industry body GSMA notes that the different types of businesses that use mobile telecommunications networks have different requirements: "One business customer, for example, may require ultra-reliable services, whereas other business customers may need ultra-high-bandwidth communication or extremely low latency."

In one way, "the most logical approach is to build a set of dedicated networks each adapted to serve one type of business customer," says the GSMA. However: "A much more efficient approach is to operate multiple dedicated networks on a common platform: this is effectively what 'network slicing' allows," and "is a radical change of paradigm compared to current implementations."[6]

Europol's document recognises the technical benefits of network slicing, but is rather more concerned with the implications for law enforcement agencies:

> *"To carry out lawful interception in the future, law enforcement will therefore require the cooperation of numerous network providers both at home and abroad. Whereas many will be subject to (national) regulation, there is also the potential of 'private slices' held by 'private third parties' that may not be subjected to such regulation. Either way, the existence of network slicing leads to potential challenges as information is fragmented, and may either not be available or accessible for law enforcement."*

Proposals for new EU legislation on "e-evidence", through which authorities in one EU member state would be able to request data directly from electronic service providers located in another member state, have already proven controversial for a number of reasons.[7] It seems that 5G technology could open up a rather similar, but much larger, can of worms.

2.2.2. Close to the edge

"Edge computing" refers to using systems at the 'edge' of computer networks to carry out functions, rather than sending data from an individual device to a centralised data system and back again. This means less latency (the time between issuing a command and receiving a response), decreased bandwidth use (as only certain data from a device will need to be sent to a centralised location for storage) and, potentially, security benefits, as certain data will

[6] GSMA, 'An introduction to network slicing', 2017, https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf

[7] 'New EU laws on e-evidence are being negotiated – but what about human rights?', *Fair Trials*, 18 April 2019, https://fairtrials.org/news/new-eu-laws-e-evidence-are-being-negotiated-%E2%80%93-what-about-human-rights

never leave a device and travel over an insecure network.[8] According to the European Telecommunications Standards Institute: "Multi-access Edge Computing (MEC) offers application developers and content providers cloud-computing capabilities and an IT service environment at the edge of the network."[9]

While this may be far more convenient and efficient than using purely centralised systems, it is decidedly inconvenient for the police. According to Europol:

> *"…devices will in the future be able to communicate directly with each other without having to use the network operator's core network. This direct communication between users leads to consequences in terms of data retrieval for law enforcement.*
>
> *Communication content and identifiers no longer have to be directed via central nodes, which means information may not be available or accessible for law enforcement."*

2.2.3. End-to-end encryption

Public debate over the default use of end-to-end encryption by popular messaging applications has been ongoing for some years. The debate is generally characterised by politicians and public officials calling for companies to facilitate access to encrypted data for law enforcement agencies, and security and technology experts responding by pointing out that doing so is impossible without introducing irredeemable security flaws.[10]

If 5G comes into widespread use, things may get even trickier for law enforcement agencies, because the international standard-setting bodies are considering making end-to-end encryption of all network communications mandatory. According to Europol's paper:

> *"While E2E [end-to-end] encryption is not yet set out as obligatory in the 5G standard, the relevant protocols are incorporated in the relevant protocol standard (Release 15). Therefore, there is a chance that E2E encryption will be included in the standard during the upcoming standardisation process (Release 16). An alternative is that terminal [i.e. device] manufacturers will (voluntarily) implement this function. Either way, E2E would make it impossible to carry out content analysis of communications within the framework of lawful interception."*

As is currently the case, it would still be possible to access telecommunications metadata on encrypted communications – the who, when and where of a phone call – but the what or why of any given communication would be far harder to discover.[11] However, accessing metadata

---

[8] Eric Hamilton, 'What is Edge Computing: The Network Edge Explained', 27 December 2018, https://www.cloudwards.net/what-is-edge-computing/

[9] 'Multi-access Edge Computing (MEC)', *ETSI*, https://www.etsi.org/technologies/multi-access-edge-computing

[10] Amie Stepanovich and Michael Karanicolas, 'Why An Encryption Backdoor for Just the "Good Guys" Won't Work', *Just Security*, 2 March 2018, https://www.justsecurity.org/53316/criminalize-security-criminals-secure/; 'Issue Brief: A "Backdoor" to Encryption for Government Surveillance', *CDT*, 3 March 2016, https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/; Bruce Schneier, 'Ray Ozzie's Encryption Backdoor', *Schneier on Security*, 7 May 2018, https://www.schneier.com/blog/archives/2018/05/ray_ozzies_encr.html

[11] It would not be impossible, however. Europol's work programme for 2019 shows that the agency's "decryption platform" was used 18 times during 2018 (from January-September), and in eight of those

may also become more difficult, given the issues raised by the encryption of IMSI codes and the introduction of "network slicing".

2.2.4. A security problem: network function virtualisation

The development of 5G networks also poses problems regarding the possibility for law enforcement agencies to maintain the confidentiality of the lists of the numbers or persons whose communications are to be monitored. The problem arises because of something called network function virtualisation. This makes it possible to use software to perform tasks that previously were done with specific pieces of hardware. While previously lists of law enforcement 'targets' may have been kept in a room at a telecoms company's offices, with restrictions on access and security checks in place, 'virtualising' the hardware traditionally used for interception tasks renders these measures obsolete.

According to Europol:

> *"This NFV means criminals can employ or execute attacks to access and even alter telephone numbers (target lists) which are to be monitored. At present there is no know [sic] commercial hardware available to prevent these attack scenarios. In addition, functions performed in one country can now be moved abroad: e.g. maintenance of mobile masts, provision of central management services (e.g. customer/user databases), thus making it (adversely) necessary to transfer lists of telephone numbers/persons to be monitored to other countries.*
>
> *The challenge therefore here, in contrast to the above mentioned challenges, is the confidentiality and the integrity of law enforcement information with respect to lawful interception, in particular the target lists."*

3. What is to be done: the law enforcement view

Both Europol and the Counter-Terrorism Coordinator (CTC) highlight various actions that national and EU authorities could take to try to deal with the looming potential obsolescence of traditional lawful interception measures. The CTC offers three "general considerations" for approaching the issue.

3.1. Setting standards

Firstly, says the CTC paper, "it may not be too late to influence standard definition. It will be important to increase the political pressure to take law enforcement concerns into account." The development of 5G technical standards is taking place in a body called 3GPP,[12] with lawful interception standards discussed in a sub-group called SA3-LI. As Europol's paper points out:

---

cases it was able to decrypt material. See: http://statewatch.org/news/2019/jun/eu-council-europol-work-programme-2019-7378-19.pdf

[12] "The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies." See: 'About 3GPP', https://www.3gpp.org/about-3gpp

> *"…a relatively small group of people represents the issue of lawful interception. For some, driving this issue is a secondary task. Therefore, there is an imbalance between 5G development and LI [lawful interception] standardisation groups. Whilst we recognise the importance of privacy and security considerations, and support these, the current approach of privacy by design allows little to no room for a balanced consideration of the law enforcement needs in the area of lawful interception to limit criminal abuse of 5G developments."*

Standards are developed through a series of documents called "releases". The 3GPP is due to publish its final release on 5G standards (Release 16) in December 2019. The CTC highlights that:

> *"Even though some technical specifications have already been frozen in the previous releases, it is still time to express law enforcement concerns. As part of Release 16, lawful interception standards will be further discussed, as well as the possibility of end-to-end encryption."*

However, the CTC warns that the 3GPP is "driven by industry interests" with voting rights dependent on financial contributions, "without veto right of authorities or unanimity principle. The votes of the companies far outweigh the votes of the law enforcement authorities, even if interests could often be aligned."

Both Europol and the CTC therefore back the idea of trying to pack more law enforcement officials into the working groups. The CTC argues that: "Increased presence of law enforcement authorities in the lawful interception sub-group [SA3-LI] would be important." Law enforcement agencies should also "keep an overall overview over what's happening in the other subgroups and on the growing role of new players other than telecoms (e.g. satellite providers, wireless carriers etc)." Specifically, the CTC suggests that the Commission take up the issue in the standardisation bodies in which it participates and that Europol consider becoming a member of both ETSI and the lawful interception subgroup of the 3GPP. Member states' authorities are also "encouraged to participate".

Legislation could be an option for meeting law enforcement demands, but "it would be preferable to incorporate the requirements already in the standards as well," concludes the CTC. Following on from this, the paper argues that law enforcement agencies should pressure companies to design networks in particular ways:

> *"Independent of standardisation, a dialogue with operators is needed to encourage them to take law enforcement and judicial concerns into account by designing specific configurations of the network."*

3.2. New laws

Given the potential difficulties with trying to influence international standard-setting bodies, the CTC considers that "legislation may also be necessary to enforce the law enforcement needs," with national legislation likely to come first. Europol's paper concurs on this point:

> "National legislative actions is [sic] therefore regarded as a priority in order to at least ensure the status quo regarding lawful interception within the framework of the ongoing

5G standardisation process *and also with a view to future technological developments."*

The member states should coordinate any legislative activity, argues the CTC, and law enforcement authorities should push national governments to take a number of issues into account:

> *"registration of all providers and obligation for all providers offering services on the territory to extract a complete and decrypted monitoring copy, to structure their network in such a way that location data is always available, to provide cooperation to ensure that technical measures such as IMSI catcher can be implemented."*

While the first of these proposals is rather unclear – it does not say what the "copy" should be a copy of, for example – it appears to imply the need for encryption 'backdoors'. If this is the case, the issue may well come onto the agenda again in the near future. As noted above, this means that civil rights groups, technologists and security experts will have to return to (or in some cases continue) informing politicians and officials precisely why no such 'backdoor' can ever work in the way they would like.

The second proposal is more straightforward, although would presumably lead to significant resistance from businesses that construct and operate telecoms network infrastructure, and perhaps from their customers, who would likely end up paying any additional costs. The third and final proposal presumably depends on the possibility for the "false-base detection" function in 5G networks to be overridden or bypassed.

The CTC also argues that a "common EU legislative framework" might be beneficial to law enforcement interests, as it could have "a stronger impact vis-à-vis the service providers," would avoid the fragmentation of standards, and could "require certain functions to be carried out within the EU," easing the possibility for retrieving data from multiple providers in non-EU jurisdictions. A common legal framework in the EU "would take time, so it is not an immediate solution," but it could:

> *"facilitate cross-border aspects of lawful/real-time interception within the EU, given that purely national interceptions today may under 5G increasingly have cross-border aspects, given the technology. While this aspect has not been covered in the draft e-evidence legislation, there may be a different urgency and hence need in the future given the future deployment of 5G."*

3.3. Police working groups

Beyond these priorities, the CTC also wants to see continuation of Europol's new working group on 5G, where "heads of telecommunications interception units" meet. According to Europol's paper, this group began in April 2018 with a "limited number of experts," but after the issue was put on the agenda of the European Police Chiefs Convention in September 2018, Germany's *Bundeskriminalamt* gave their backing to the initiative and a second, larger meeting took place in February 2019. The CTC suggests that Eurojust and national telecoms companies could be invited to participate in the working group.

There is also a need for law enforcement and judicial authorities to engage with cybersecurity bodies, as "cybersecurity concerns might sometimes be conflicting with law enforcement

concerns" – for example, demands for the encryption of data versus demands for its ready availability.

The CTC and Europol both want to see more discussions in EU institutions. Europol notes the role of the Commission and the Council Presidency and the need for "mutual exchange at the level of the European security authorities," but also beyond, "with international co-operation partners such as the USA, CAN [Canada] and AUS [Australia]." The CTC highlights the need to take the issue to the Council's internal security committee (COSI) and ultimately to the Justice and Home Affairs (JHA) Council. In fact, it seems the JHA Council will discuss the issue in the coming days – "Implications of 5G in the area of internal security" is on the agenda for 11:30 on Friday 7 June.[13]

4. Out with the old, in with the new

While it seems clear that the introduction of 5G technology will make certain 'traditional' law enforcement measures more difficult – or perhaps even obsolete – neither Europol or the Counter-Terrorism Coordinator give consideration, in these documents, to other changes that the technology will supposedly introduce. If the hype around 5G networks is to be believed, one of its main functions will be to make possible the generation, storage and sharing of vast tomes of data on individuals, objects, devices and the environment through the 'internet of things'. This essentially involves placing sensors and wireless networking technology in pretty much anything you can think of,[14] and connecting it to the internet.

In March 2015, Gunther Oettinger (at that time the European Commissioner for Digital Economy and Society) expounded upon the potential wonders of 5G to the audience at the Mobile World Congress trade fair in Barcelona. In his speech, he argued that 5G will become "THE infrastructure. Everybody and everything will use 5G. Anywhere, at any time, and on the move, always best connected with almost zero delay and a perceived limitless capacity." Europe is apparently at the forefront of the "journey towards this bright 5G future," in which the network will be as "pervasive as the air we breathe, one that can be used for all sorts of different and personalised usages." In this vision, everything will be connected to everything, all the time: "From fridges to heating. From hospitals to factories. Any industry" – and presumably every person – "will need to adjust to this new reality."[15]

Law enforcement officials and agencies have long-taken a keen interest in these looming technological developments. In 2007, a "concept paper" written by Portuguese officials argued that the number of "digital traces" created by individuals "is likely to increase by several orders of magnitude in the next ten years."[16] The final report that followed argued that "in an

---

[13] Council of the EU, 'Indicative programme - Justice and Home Affairs Council of 6 and 7 June 2019', https://www.consilium.europa.eu/en/press/press-releases/2019/06/04/indicative-programme-justice-and-home-affairs-council-of-6-and-7-june-2019/

[14] Some more mundane 'innovations' unveiled in recent years include "smart" (i.e. embedded with sensors and Wi-Fi-enabled) toothbrushes, toilets, ovens and scales.

[15] Gunther Oettinger, 'The road to 5G', speech given at the Mobile World Congress, Barcelona, 2 March 2015, http://europa.eu/rapid/press-release_SPEECH-15-4535_en.htm

[16] 'Concept paper on the European strategy to transform Public security organizations in a Connected world', p.8, http://www.statewatch.org/news/2008/jul/eu-futures-dec-sec-privacy-2007.pdf

increasingly connected world… public security organisations will have access to almost limitless amounts of potentially useful information."[17]

More recently, the Police Foundation ("the UK's policing think tank") has made similar arguments. The internet of things "is going to change the game when it comes to police investigations," although accessing the vast amounts of data generated in this brave new world presents "a potentially massive challenge for the police in terms of workload."[18] A 2016 paper written by academics, civil society organisations and US intelligence officials and published by Harvard University's Berkman Center argued that:

> *"If the Internet of Things has as much impact as is predicted, the future will be even more laden with sensors that can be commandeered for law enforcement surveillance; and this is a world far apart from one in which opportunities for surveillance have gone dark. It is vital to appreciate these trends and to make thoughtful decisions about how pervasively open to surveillance we think our built environments should be – by home and foreign governments, and by the companies who offer the products that are transforming our personal spaces."*[19]

Companies are of course on hand to help law enforcement agencies adjust to these developments. Cellebrite, a major manufacturer of mobile phone data extraction systems used by police forces around the world, boasts of "digital forensics solutions" that are "powered by AI and machine-learning to assist law enforcement to scale procedures, automate tasks and eliminate manual review of digital evidence."[20]

It is clear that the number of "digital traces" generated by individuals living in industrialised (or post-industrial) western societies has massively increased in the last decade, and it will continue to do so in the future. Europol and the CTC are well aware of this fact, and they no doubt have their reasons for not raising this point in their papers. However, the very same technology that they argue must be more tightly regulated by government in order to maintain 'traditional' surveillance tactics will also introduce the possibility of far more novel and invasive techniques.

On this point, the Berkman Center study argued that "the increasing prevalence of networked sensors in machines and appliances point to a future with more opportunities for surveillance, not less." The implications of this are raised in the previously-cited Police Foundation paper, which argued that "accessing data via devices linked to specific individuals may involve major invasions of privacy and a fundamental, and at this stage unregulated, shift in the relationship between the police and the public."

---

[17] Tony Bunyan, 'The "digital tsunami" and the EU surveillance state', March 2009, http://www.statewatch.org/analyses/no-75-digital-tsunami.pdf

[18] Ian Kearns and Rick Muir, 'Data-driven policing and public value', *The Police Foundation*, March 2019, http://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/data_driven_policing_final.pdf

[19] Urs Gasser et. al., 'Don't Panic: Making Progress on the "Going Dark" Debate', *The Berkman Center for Internet & Society at Harvard University,* 1 February 2016, https://cyber.harvard.edu/pubrelease/dont-panic/

[20] Ariel Watson, 'How 5G Challenges and Benefits Law Enforcement', *Cellebrite*, 28 February 2019, https://www.cellebrite.com/en/blog/how-5g-challenges-and-benefits-law-enforcement/

5. The need for public debate

In the USA, the issue of data gathered by 'smart' devices being made accessible to law enforcement agencies has been raised in a number of cases in recent years. In November 2018, a court ordered that Amazon provide the police with recordings from one of its Echo devices, as part of a murder investigation.[21] Two years previously, police demanded access to Echo data as well as that from a "smart water meter", believing that a murder suspect cleaned up the scene "because of the amount of water he used in a two-hour window."[22]

In the same year, access to data from a man's pacemaker made it possible to charge him with arson and insurance fraud, and in 2015 authorities in Pennsylvania "dismissed rape charges after data from a woman's Fitbit contradicted her version of her whereabouts during the… alleged assault."[23] Indeed, as far back as 2003, a US court overturned a ruling that allowed the FBI to use an in-car safety system as a listening device on the grounds that doing so required disabling the safety features of the system, but the decision left the door open for wiretapping in-car audio devices.[24]

On this side of the Atlantic, such issues have not yet come to public prominence, but there are long-standing debates over the limits of police powers regarding access to telecommunications and device data. In the UK, groups such as *Privacy International* and *Big Brother Watch* have also raised the issue of warrantless extraction of data stored within mobile phones,[25] while groups across the EU continue to campaign on numerous surveillance issues. More broadly, important legal standards on data retention have been set through court cases brought by campaigning groups and individuals[26] (although national governments still hope to re-introduce EU-wide rules[27]) and in the last few years new EU data protection laws have been put in place, including measures on data protection in the policing and criminal justice sector. It is, however, an open question whether these frameworks will be sufficient in the light of potential future developments.

If there is to be an increase in the presence of representatives of police forces and interior ministries in policy and standard-setting discussions, will there also be a call for greater

---

[21] Chavie Lieber, 'Amazon's Alexa might be a key witness in a murder case', *Vox*, 12 November 2018, https://www.vox.com/the-goods/2018/11/12/18089090/amazon-echo-alexa-smart-speaker-privacy-data

[22] Kathryn Gilker, 'Bentonville Police Use Smart Water Meters As Evidence In Murder Investigation', *5News*, 28 December 2016, https://5newsonline.com/2016/12/28/bentonville-police-use-smart-water-meters-as-evidence-in-murder-investigation/

[23] Rob Lever, 'Secrets from smart devices find path to US legal system', *Phys.org*, 19 March 2017, https://phys.org/news/2017-03-secrets-smart-devices-path-legal.html

[24] Adam Liptak, 'Court Leaves the Door Open For Safety System Wiretaps', *The New York Times*, 21 December 2003, https://www.nytimes.com/2003/12/21/automobiles/court-leaves-the-door-open-for-safety-system-wiretaps.html

[25] 'Push this button for evidence', *Privacy International*, 16 May 2019, https://www.privacyinternational.org/news-analysis/2901/push-button-evidence; ' Victims Not Suspects', *Big Brother Watch*, https://bigbrotherwatch.org.uk/all-campaigns/victims-not-suspects/

[26] For example, the *Digital Rights Ireland* case in the Court of Justice of the EU and the *Tele2/Watson* case in the European Court of Human Rights.

[27] 'Council of the EU wants data retention without cause - Germany joins in', *Statewatch News*, 29 May 2019, http://statewatch.org/news/2019/may/eu-council-data-retention.htm

participation from officials responsible for ensuring control and oversight of those bodies? Combined with ongoing plans to enact interoperability and unify databases on the basis of the "principle of availability", shaping technological advances to suit police purposes could significantly increase the possibility for state agencies across the EU to access detailed and intimate information on individuals. The implications for social control are considerable.

Even if the hype about 5G networks and the internet of things is overblown, there is a need for broader discussion about the possibilities that new technologies offer for surveillance not only by private companies, but by public authorities. The demands of bodies such as Europol and the CTC regarding traditional telecoms interception and 5G technology should be seen in this context and should, moreover, be a matter for public deliberation. The issues they raise might serve as a useful starting point for wider debates about the vast, dangerous surveillance possibilities that 5G and related technologies make possible.

Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 18 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness.

One of Statewatch's primary purposes is to provide a service for civil society to encourage informed discussion and debate - through the provision of news, features and analyses backed up by full-text documentation so that people can access for themselves primary sources and come to their own conclusions.

Statewatch is the research and education arm of a UK registered charity and is funded by grant-making trusts and donations from individuals.

Web: www.statewatch.org | Email: office@statewatch.org | Phone: (00 44) 203 691 5227

Post: c/o MDR, 88 Fleet Street, London EC4Y 1DH

Charity number: 1154784 | Company number: 08480724
Registered office: 2-6 Cannon Street, London, EC4M 6YH