First statement of Silke Holtmanns
15 April 2019

**IN THE FIRST TIER TRIBUNAL
GENERAL REGULATORY CHAMBER
(INFORMATION RIGHTS)**

Appeal nos: EA.2018.0164 and 0170

BETWEEN:

PRIVACY INTERNATIONAL

Appellant

-and-

(1) THE INFORMATION COMMISSIONER'S OFFICE

(2) COMMISSIONER OF THE METROPOLITAN POLICE

(3) POLICE AND CRIME COMMISSIONER FOR WARWICKSHIRE

Respondents

FIRST WITNESS STATEMENT OF SILKE HOLTMANNS

I, Dr. Silke Holtmanns, [redacted] say as follows:

INTRODUCTION

1. I hold a PhD in Mathematics from the University of Paderborn, Germany. I have worked for 19 years in mobile communication security. I have authored over 100 publications on mobile network and phone security and hold over 100 patents in this area. I am the editor of 11 technical mobile security specifications for key standardization bodies which are used around the world.[1] I am currently a Security Expert and Distinguished Member of Technical Staff working for Nokia Oy in Finland in Security Research, where I present security challenges and solutions to mobile network operators, governments (e.g. the European Union Agency for Network and Information Security, and the Federal Communications Commission of the United States), and large security events like DefCon or Blackhat. This witness statement is provided in my personal capacity and not

[1] As editor, I coordinate development of the specification, including by combining and structuring inputs from various contributors. I also integrate changes to the specification and make corrections where necessary, together with the standardisation body.

in my capacity as a Nokia employee.

2. I make this statement in relation to the appeal to the First-tier Tribunal by the Appellant challenging the Information Commissioner's Office's decisions upholding various public bodies' refusals to confirm or deny the existence of records responsive to Freedom of Information Act requests about the purchase and use of IMSI catchers.

3. This witness statement will address what an IMSI catcher is, how it operates, and what the impact is for mobile phone users.[2] An IMSI catcher is a surveillance tool, which can impact both the target of the surveillance as well as bystanders in the vicinity, e.g. by collecting IMSI/IMEI data or by blocking access to emergency calls. In comparison to more traditional surveillance methods, where authorised government officials could obtain similar data directly from the mobile operator for a specific target, IMSI catcher activities are less traceable in terms of how they operate and what persons, including bystanders, have been affected.

4. Where the contents of this statement are within my knowledge, I confirm that they are true; where they are not, I have identified the source of the relevant information, and I confirm that they are true to the best of my knowledge and belief.

WHAT IS AN IMSI AND WHY IS IT IMPORTANT?

5. Every person who wishes to use a mobile phone must purchase a little card commonly known as a subscriber identity module ("**SIM**") card from a mobile phone operator.[3] Many mobile phone users also sign a service contract, known as a 'subscription', to which a phone number is typically attached. The phone number is known as the Mobile Station International Subscriber Directory ("**MSISDN**").

6. The International Mobile Subscriber Identity ("**IMSI**") is a unique number bound to a SIM card. The IMSI contains a country identifier, a mobile network identifier and the mobile

[2] This statement addresses the operation of IMSI catchers on 2G, 3G and 4G networks, i.e. the network technologies that are currently in use by mobile network operators. It does not cover future networks, such as 5G.

[3] I use the term 'SIM card' throughout this statement to refer to the card that stores the IMSI and is used to identify and authenticate subscribers on mobile phones. However, technically speaking, SIM cards are used on 2G networks, whereas for 3G and 4G networks, it is a 'universal integrated circuit card' ("**UICC**") with SIM and/or 'universal subscriber identity module' ("**USIM**") applications. Most cards today will be UICC with SIM and UISM applications.

subscription identifier.[4] Because the IMSI identifies the mobile subscription, it therefore identifies the mobile user uniquely across the world. In this sense, the IMSI is like a social identity number or a passport number, where an individual is identifiable by a unique number.

7. The IMSI is stored in the SIM card, but it is available to the phone software. As a user you may not be able to retrieve the IMSI, but it is there and it is used for communication. The IMSI does not change during the lifetime of your SIM card and it is stored by the operator as part of its operational procedures.

8. In addition, every phone has an International Mobile Equipment Identity ("**IMEI**"), which is a number that uniquely identifies the phone (rather than the SIM card), i.e. indicating the type and serial number of the phone.

9. Since the IMEI is a unique number bound to the phone, if you buy a new phone and put in your old SIM card, then the IMEI (i.e. phone identifier) would change, but your IMSI (i.e. subscription identifier) would remain the same.

10. A mobile phone network is a very complex system, requiring different servers to communicate with each other to enable various services. These servers include charging servers, which enable communications service providers to charge their customers; mobility management nodes, which enable tracking of subscribers and delivery of calls and other mobile phone services; and base stations, which connect mobile phones to the network. In order for servers to communicate with each other, they must first identify a subscription and the related service contract and arrangements (e.g. if you only have access to the 2G network or to the 4G network and at what rates) via the IMSI.

WHAT IS AN IMSI CATCHER?

11. An IMSI catcher, also called a 'stingray' or 'false base station', is a small mobile base station. IMSI catchers vary in size, range, capabilities and price. The first basic IMSI

[4] A mobile subscription can also be a 'data only' subscription, e.g. for an 'Internet of things' device (i.e. a device with internet connectivity), like a connected car. A data only subscription would not necessarily have an MSISDN (phone number), but it will have an IMSI. Without an IMSI, the mobile network operator would not be able to charge the subscriber or provide mobile network services. Dual SIM card phones (i.e. phones with two SIM card slots) usually have two IMSIs, one for each SIM card.

catcher was manufactured by Rohde & Schwartz in 1996.[5]

12. The IMSI catcher pictured below,[6] when equipped with a cover and an antenna, has the size and 'look' of a Wifi access point and can be obtained easily for research purposes from the Internet. The equipment required for this IMSI catcher to function – i.e. radio hardware, antennas, and a good laptop – will cost about £2,500. The software is open source, and is accessible through the OpenBTS software project, for example.

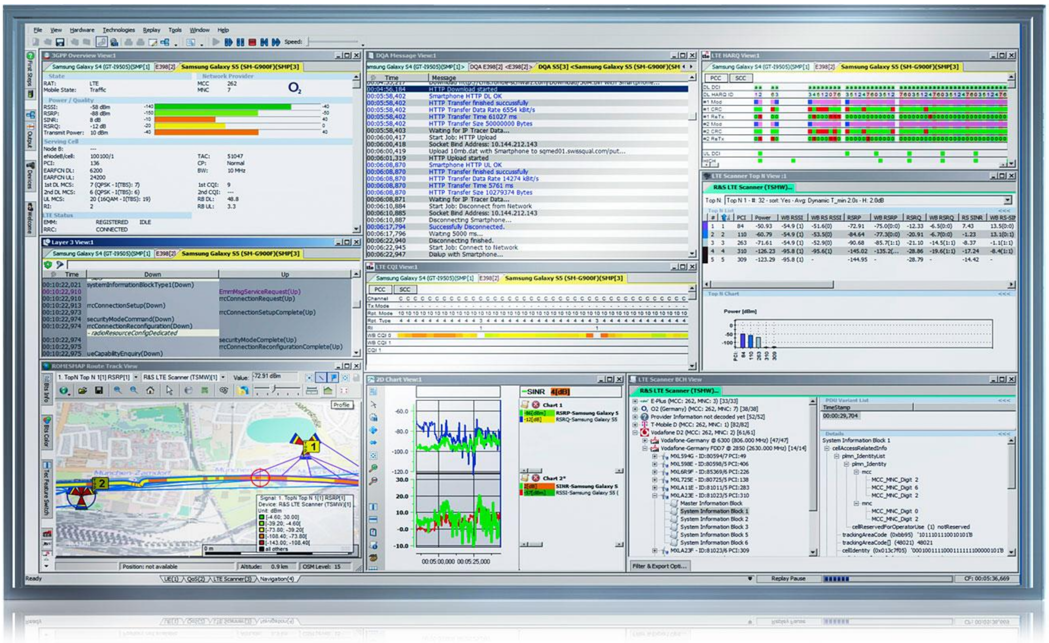
USRP B210 (Board Only)

[5] *See* Lisa Parks, Rise of the IMSI Catcher, Media Fields Journal no. 11, 2016, pp. 2-3 (citing Daehyun Strobel, "IMSI Catcher", Seminararbeit Ruhr-Universität Bochum, 13 July 2007, https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf), available at https://www.academia.edu/29059675/Rise_of_the_IMSI_Catcher (last accessed 8 April 2019); *see also* Holger Dambeck, IMSI-Catcher zur Mobilfunküberwachung bald legal, Heise Online, 20 Nov. 2001, https://www.heise.de/newsticker/meldung/IMSI-Catcher-zur-Mobilfunkueberwachung-bald-legal-46391.html (last accessed 8 April 2019).

[6] This image is also available at Ettus Research, Product Categories, USRP Bus Series, USRP B210 (Board Only), https://www.ettus.com/product/details/UB210-KIT (last accessed 8 April 2019).

13. The IMSI catcher pictured below[7] is an example of a more advanced model, which is more likely to be used by police forces operationally.

14. The image below[8] captures the user interface of this IMSI catcher. The middle upper box documents mobile activity.



```
Time          Message
00:04:56,184  HTTP Download started
00:05:58,402  Smartphone HTTP DL OK
00:05:58,402  HTTP Transfer finished successfully
00:05:58,402  HTTP Transfer Data Rate 6554 kBit/s
00:05:58,402  HTTP Transfer Time 61027 ms
00:05:58,402  HTTP Transfer Size 50000000 Bytes
00:05:58,403  Waiting for IP Tracer Data...
00:06:00,417  Start Job: HTTP Upload
00:06:00,418  Socket Bind Address: 10.144.212.143
00:06:00,419  Upload 10mb.dat with Smartphone to sqmed01.swissqual.com/put...
00:06:01,319  HTTP Upload started
00:06:08,870  Smartphone HTTP UL OK
00:06:08,870  HTTP Transfer finished successfully
00:06:08,870  HTTP Transfer Data Rate 14274 kBit/s
00:06:08,870  HTTP Transfer Time 5761 ms
00:06:08,870  HTTP Transfer Size 10279374 Bytes
00:06:08,871  Waiting for IP Tracer Data...
00:06:10,884  Start Job: Disconnect from Network
00:06:10,885  Socket Bind Address: 10.144.212.143
00:06:10,887  Disconnecting Smartphone...
00:06:17,794  Successfully Disconnected.
00:06:17,796  Waiting 5000 ms...
00:06:22,940  Disconnecting finished.
00:06:22,945  Start Job: Connect to Network
00:06:22,947  Dialup with Smartphone...
```

[7] This image is also available at Rohde & Schwarz, Products, Test and Measurement, Mobile Network Testing, R&S®ROMES4 Drive Test Software, https://www.rohde-schwarz.com/ph/product/romes-productstartpage_63493-8650.html (last accessed 8 April 2019).

[8] This image is also available at Rohde & Schwarz, Products, Test and Measurement, Mobile Network Testing, R&S®ROMES4 Drive Test Software, https://www.rohde-schwarz.com/ph/product/romes-productstartpage_63493-8650.html (last accessed 8 April 2019).

How Do IMSI Catchers Work?

Passive v. Active Modes

15. An IMSI catcher can act in either a passive mode or an active mode. The operator of the IMSI catcher chooses which mode to use.

16. In the passive mode an IMSI catcher checks which mobile towers are within its vicinity and it may, by tuning into a particular base station, intercept mobile phone data travelling between the phone and that base station.

17. In the active mode, the IMSI catcher acts as what is called a 'man-in-the-middle' in the communication path by presenting itself as a base station amid the mobile phone network. By presenting itself as a base station emitting the strongest signal, it entices mobile phones within its vicinity to connect to it and forces them to transmit data, in particular their IMSI and IMEI.

18. In order to enable connection with phones within its vicinity, the IMSI catcher first obtains certain security information from those phones.[9] Once it has obtained that information, it can use the information to pretend that it is itself a mobile phone and connect to the real mobile phone network. In this way, the IMSI catcher presents itself to the phone as the real network, while presenting itself to the real network as the phone, and in the process serving as a bridge (i.e. the man-in-the-middle) between the phone and the real network.

19. Once a phone has connected to an IMSI catcher (explained in further detail below, see paragraphs 23 to 27), it becomes possible to monitor the operations of the phone, i.e. to see all communications and data going to and from the network, such as calls and messages (e.g. password reset text messages).[10] Activities that happen 'in the device only' (i.e. without needing to connect to the network) are not visible to the IMSI catcher,

[9] The exact process of connecting to the IMSI catcher, which requires the transmission of several messages between the phone and the IMSI catcher in addition to other elements, is beyond the scope of this statement. For further details on this process, see Joseph Ooi, School of Engineering and Applied Science, University of Pennsylvania, "IMSI Catchers and Mobile Security", 29 April 2015, available at https://www.cis.upenn.edu/current-students/undergraduate/courses/documents/EAS499Honors-IMSICatchersandMobileSecurity-V18F-1.pdf (last accessed 8 April 2019).

[10] If the user is using a service with application layer encryption, e.g. WhatsApp, then the IMSI catcher cannot see 'into' that encrypted data. Application layer encryption means that the application you are using, such as WhatsApp, first encrypts the data prior to transmitting it across a network. Application layer encryption is distinguishable from transport layer encryption, which encrypts the data in transit, so that it is indecipherable if intercepted.

but today most activities we perform on our phone require network connectivity. An activity that happens ‘in the device only’ might be a photo taken and stored on the phone (so long as the photo is not transmitted over the mobile phone network, e.g. by posting it on a social media site or as part of a back-up to a cloud server). Activities that we perform on our phone requiring network activity would include any internet searches, map searches, or even financial transactions through banking apps.[11]

20. Some IMSI catchers can also, by virtue of acting as a man-in-the-middle, change the content of communications and data or prevent them from being transmitted. In other words, they may capture a message from the phone, which believes it is sending it to the real network, and either replace that message with a new one before transmitting it onwards to the real network or not transmit it to the real network at all.

21. The remainder of the section will focus on how an IMSI catcher works in the active mode.

How Does a Phone Connect to an IMSI Catcher?

22. Suppose you are travelling abroad to Iceland. You land and switch on your mobile phone. Your phone then contacts the mobile networks around it.

23. The mobile networks operating in Iceland need to recognise your subscription and which operator that subscription belongs to. For that reason, the mobile phone will send its IMSI (and IMEI) to requesting networks. The IMSI contains a mobile country code and a mobile network code, so the Icelandic operator can check which operator your subscription is with and if they have a roaming agreement with that operator.

24. Most default settings in mobile phones make the determination of network choice automatic. A phone will try to attach itself to a network that is on the preferred partner list of the home operator of the user and if there are several, it will connect to the one with the strongest signal. For example, if your phone sees the home network (i.e. the operator from which you have bought the subscription) and a ‘roaming network’ and the

[11] Today, many websites (like Google) and banking applications use an additional security layer to protect the transmission of data on top of the mobile network security. Where an additional security layer exists, the IMSI catcher would not be able to read the data transmitted to and from the mobile network (it would be able to see that the phone is transmitting data to and from the network but it would be unable to see what that data is). However, there are still many websites and applications that do not use any additional security layer.

roaming network has a very strong signal, it will connect to the roaming network. Once accepted and connected to a network, the phone tries not to change networks, as it would break ongoing data sessions or calls. But if it has no connectivity or its connection to a network is very weak, it will try to find another network (although the specific rules for this process are dependent on the mobile phone).

25. An IMSI catcher in active mode has two possibilities in terms of its operation:

   a. It will present itself as part of the home network of the user, i.e. the mobile phone will believe the IMSI catcher is part of its normal network and that the operator has just set up a new base station (which is a normal occurrence); or

   b. It will either try to show an unknown network to the phone, i.e. as if the user is travelling (although the phone is then likely to stay with its home network), or it will present itself as part of a different network. In these scenarios, the user may notice that the phone is connected not to the home network but to a different network (the network the phone is connected to is usually shown on the home screen). These approaches usually point to a badly configured IMSI catcher.

26. To ensure that a mobile phone does not 'accidentally' connect to a real network, an IMSI catcher can transmit to phones an empty list of neighbouring cells or 'block' ('yam') the frequencies of real operators in a small geographic area. In yamming the frequency, the IMSI catcher would block the frequencies of real operators for all users in its vicinity and prevent them from accessing services, including both normal and emergency calls.

2G v. 3G and 4G Networks

27. During the design of 2G GSM (Global System for Mobile communications) networks it was assumed that it would be very difficult and expensive to pose and impersonate the network. Therefore, for these networks, while the mobile phone has to prove its identity (i.e. that the phone attempting to access the network has a valid subscription), the network does not need to prove to the phone that it is the real network with which the user has a contract. However, 3G and 4G networks operate differently, in that the mobile phone has to prove its identity to the network *and* the network must also prove its identity to the mobile phone. But depending on the particular coverage in an area, a phone may switch from a 3G/4G network to a 2G network, if the connection to 3G/4G is

too weak or not available at all.

28. Because 3G and 4G networks authenticate themselves, i.e. prove to a connecting phone that they are the real home network of the user, the main attack vector for IMSI catchers is to force a phone connecting to it to downgrade to the 2G network. A phone will notice this change 'deep in the phone', i.e. the baseband chip, which is usually not directly accessible to the user, will manage this change. However, many phones do also display what network they are currently using.[12]

29. Depending on the phone, it is possible to set network preferences, e.g. to 3G or 4G. But if a phone with a 3G/4G preference does not see either network, it will still connect to a 2G base station. With most phones, this setting is just a preference and it usually will not be a defence against the operation of an IMSI catcher.

30. It is normal for mobile operators to continue to operate 2G base stations as part of their network. For example, some operators use the 2G base stations for Internet of Things ("**IoT**") devices, e.g. cars with network connectivity, wearable devices like fitness trackers and health monitors, 'smart' home devices like thermostats, plugs and locks. Because those device subscriptions are relatively cheap, the operators often believe there to be a good return on investment if they move those subscriptions to the 2G network. IMSI catchers operate on IoT devices in the same way that they operate on mobile phones. In other words, those devices when attempting to connect to the mobile phone network in order to transmit communications or data (e.g. a car making an emergency call, a health monitor sharing out-patient care data, a home security device sending an alert about unusual activity) will instead transmit their IMSI data to an IMSI catcher. The IMSI catcher may then monitor and intercept communications and data between those devices and the real network and even potentially manipulate such communications and data.

No-Encryption Algorithms

31. Mobile phone networks can protect data by encrypting it as it is transmitted over the network. However, all mobile phones support a no-encryption 'algorithm', which permits

[12] It is also possible for an IMSI catcher to falsely present as a 3G or 4G base station and then when a phone connects to it, to downgrade the phone to the 2G network. However, that would require the use of additional capabilities, namely hacking, in addition to the IMSI catcher.

the phone to transmit data unencrypted over the air to the base station. When a phone connects to a base station, including an IMSI catcher, the base station determines which security algorithms to use for the transmission of data. An IMSI catcher would select a no-encryption algorithm in order to ensure the data is not protected and can be seen. The phone would obey the command from the base station and transmit data to it unencrypted.

USING AN IMSI CATCHER IN THE FIELD

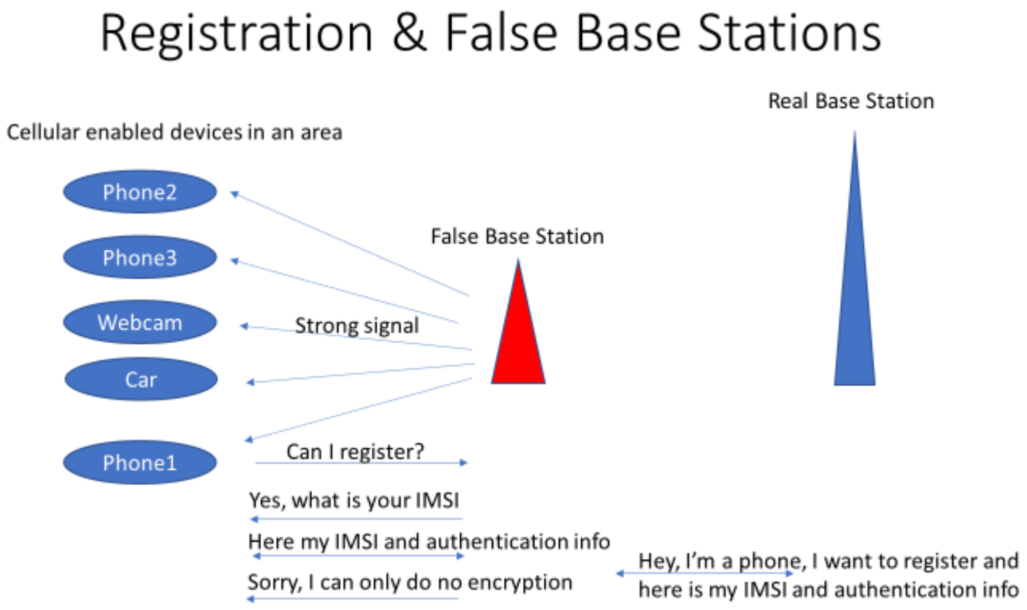
32. An IMSI catcher can be used to 'catch all' devices within its given vicinity, which is a common default setting when installing typical IMSI catcher software.

33. An IMSI catcher can also be used to target a particular mobile phone user, in which case you would need to know that user's IMSI. But even in this scenario, all other phones in the vicinity of the IMSI catcher would attempt to connect to it. When trying to connect to the IMSI catcher, these phones would transmit their IMSI and potentially IMEI data (depending on the network protocol used), which would be retained in the logs of the IMSI catcher. If properly configured, the IMSI catcher would reject the connection attempt by the phones of non-targeted users. But there remains a risk, dependent on the configurations of the IMSI catcher and the skill of the person configuring it, that the phones of non-targeted users will successfully connect to the IMSI catcher and have their communications and data compromised, in addition to being unable to make calls, including emergency calls.

34. If you wanted to find a specific person and did not know the IMSI in advance, the IMSI catcher could be operated by capturing all IMSIs within geographic locations where the target might be, e.g. at work and at home. Then you would compare the two sets of IMSIs (i.e. IMSIs from the target's work location and the target's home location) and try to make a match by seeing which IMSIs appear in both places. Alternatively, the entity operating the IMSI catcher could take the captured IMSIs and request all user information associated with this data. Once it has obtained this list of users, it could cross-check to see if the target was on that list. There exist services that provide such user information at the request of the government upon presentation of IMSI or IMEI data (e.g. National Mobile Property Register, https://thenmpr.com/home). In other words, it is a small step to use information obtained using the IMSI catcher, such as the IMSI, to

arrive at the 'real user'. This approach would result in the tracking of many bystanders, i.e. the IMSI catcher would capture their IMSI (and potentially IMEI), location information and device type.

35. The figure below depicts the use of an IMSI catcher to target a specific phone – Phone1. However, all devices in the vicinity of the IMSI catcher (i.e. Phone2, Phone3, Webcam and Car) would see the IMSI catcher as 'the real thing', i.e. a real base station. They would therefore also try to connect and register with the IMSI catcher. In that process, they would all transmit their IMSI and potentially IMEI to the IMSI catcher.



Registration & False Base Stations

Real Base Station
Cellular enabled devices in an area
Phone2
Phone3
Webcam
Car
Phone1
False Base Station
Strong signal
Can I register?
Yes, what is your IMSI
Here my IMSI and authentication info
Sorry, I can only do no encryption
Hey, I'm a phone, I want to register and here is my IMSI and authentication info

36. If properly configured, the IMSI catcher would only allow Phone1 to connect as that is the target. In order to enable connection with Phone1, the IMSI catcher would obtain certain security information from Phone1. Then it would take that information, pretend that it was itself the mobile phone and connect to the real network, thereby performing a so-called man-in-the-middle attack. As part of this process, it may also mean that other devices in the vicinity of the IMSI catcher might be temporarily out of service, i.e. unable to connect to a real base station.

WHAT RISKS DO IMSI CATCHERS POSE TO USERS?[13]

37. IMSI catchers pose a number of risks to mobile device users, including users of IoT devices:

a. Capture of data about the device and user, including IMSI and potentially IMEI data and potentially other device information (e.g. software version);

b. Location tracking of a target mobile phone user, but also of bystanders (even in the course of tracking a target user), through the capture of data about the device;[14]

c. Interception of communications and data, i.e. the IMSI catcher acts as a man-in-the-middle between the phone and the real network and by that means has access to all of the information that goes via that bridge;

d. Changing the content of communications and data or preventing communications and data from transmitting to and from the real network;

e. Potential lack of service, including to make emergency calls, both through yamming and because the IMSI catcher acting as a man-in-the-middle would need to build a bridge to the real network for each connected user and that may present a load demand for the IMSI catcher;

f. Loss of communications confidentiality if the IMSI catcher chooses a 'no encryption' algorithm.

Indirect Threats to Users Posed by IMSI catchers

38. Once captured, a user's IMSI can be misused for other purposes. (Remember that a mobile phone user's IMSI tends to stay the same, even if the user buys a new phone, as

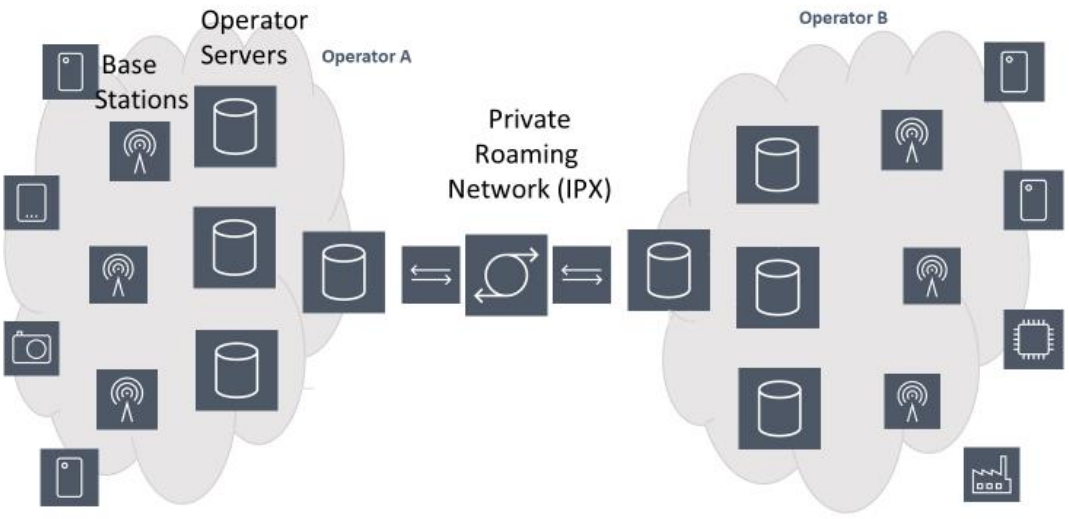
[13] This statement provides only a brief overview of IMSI catchers and their impacts. For a more detailed description of the technical details underpinning IMSI catcher attacks and their impacts, see Joseph Ooi, School of Engineering and Applied Science, University of Pennsylvania, "IMSI Catchers and Mobile Security", 29 April 2015, available at https://www.cis.upenn.edu/current-students/undergraduate/courses/documents/EAS499Honors-IMSICatchersandMobileSecurity-V18F-1.pdf (last accessed 8 April 2019).

[14] Once a mobile device has revealed its IMSI, an IMSI catcher can determine its general location by measuring the strength of the signal from the phone. Moving the IMSI catcher around and measuring the strength of the signal from different locations permits a more precise triangulation of the phone's location.

the old SIM card is commonly used. This means that IMSIs have a long life, and once captured can therefore continue to be misused for a long time.)

39. Different mobile phone operators connect to each other through networks called interconnection networks, such as the Internetwork Packet Exchange ("**IPX**"). These networks are used, for example, to enable roaming, which allows a user traveling abroad to 'roam' on a network that is not his or her home network. The image below depicts how two operators would enable roaming to occur. These interconnection networks were initially built as small private networks between mobile operators and therefore lacked proper security protection. Today, interconnection networks include more than 2000 companies from countries all over the world, ranging from the U.K. and the U.S. to China and North Korea. Less trusted entities may also use this network not with the intent of providing roaming services but also as a means of attacking individuals.

Two Mobile Operator Networks Connect



40. When an entity such as the government collects IMSI data, there are numerous risks, including that the data could be lost or fall into the wrong hands. So, for example, a foreign government or company, by obtaining IMSI data, could then use their access to the interconnection networks to track users through their IMSI or to eavesdrop or otherwise interfere with those persons' communications.

41. These risks can have a national security impact as well. If the police were to use an IMSI catcher within the vicinity of a government building, the IMSI catcher might collect the IMSI data of all of the people working in that building, potentially including politicians and high-level officials. That IMSI data could be misused by the government itself or by a third party to track those individuals or to facilitate other surveillance against them.

42. Criminals can also use IMSI data and their access to the interconnection networks to facilitate cybercrime. For example, many of us use confirmation codes, also known as 'two-factor authentication', to authenticate our communications with banks and commercial platforms when receiving services from them through our mobile phones. With IMSI data and access to the interconnection networks, criminals can intercept confirmation codes sent via SMS messages and access user accounts.[15]

Methods for Detecting IMSI Catchers

43. There exist certain methods for detecting the use of IMSI catchers, for example by observing network anomalies or a strange handover between base stations. However, some of the signs that an IMSI catcher is in use may also be signs that a network is configured badly. A mobile network is a very complex entity, so the configuration of it might not be optimal and there might be dropped calls or similar problems due to erroneous configuration. So it is unclear how effective methods for detecting IMSI catchers are as it is not easy to differentiate between misconfigurations and IMSI catcher activities.

44. The details of radio handovers (i.e. the mobile device switching between base stations) lie deep in the phone in the baseband chip and are not easily accessible to the user from the phone. However, there do exist several applications that a mobile phone user can download to their phone, which process the information from the baseband chip and detect strange network activity. These applications include SnoopSnitch,[16] CellSpyCatcher,[17] AIMSCID and Dashak. The reliability of the warning message

[15] See, e.g., Chris Bing, "It Finally Happened: Criminals Exploit SS7 Vulnerabilities, Prompting Concerns About 2FA", Cyberscoop, 8 May 2017, https://www.cyberscoop.com/finally-happened-criminals-exploit-ss7-vulnerabilities-prompting-concerns-2fa/ (last accessed 8 April 2019).

[16] https://play.google.com/store/apps/details?id=de.srlabs.snoopsnitch&hl=en (last accessed 8 April 2019).

[17] https://play.google.com/store/apps/details?id=com.skibapps.cellspycatcher (last accessed 8 April 2019).

produced by these 'detection apps' varies and depends on how well the network is configured and maintained or if it has a lot of technical issues like broken calls, and also on how well the IMSI catcher is configured to avoid detection.

46. In addition, as the data pertaining to network activity resides deep in the phone, those apps have to be run on a rooted phone, i.e. the phone must permit the user to attain privileged control over various subsystems of the phone, making the phone potentially vulnerable to malware.

Statement of Truth

I believe that the facts stated in this witness statement are true.

[redacted]

Silke Holtmanns

Dated this ..15th.. day of April 2019