Baker McKenzie.

2017 Surveillance Law Comparison Guide

2017

Baker McKenzie's Global Surveillance Survey

2017

Baker McKenzie's 2017 Global Surveillance Survey

One year ago, in April 2016, Baker McKenzie published its first global surveillance survey - with overview heat maps and detailed questions and answers for 39 jurisdictions worldwide. A year later, the basic picture has not dramatically changed: Most countries are conducting surveillance and espionage to protect their national security - while at the same time opposing surveillance and espionage by other countries. But, some details have changed since details regarding the U.S. NSA program were leaked in 2013: Germany, Russia, the United Kingdom and a few other European jurisdictions have updated their surveillance, data residency and retention laws in the interest of increased national security - while the United States have enacted additional privacy protections and gradually scaled back their surveillance programs.

Recall that in 2015, the Court of Justice of the European Union (CJEU) raised the question of whether the level of data protection in the US is adequate and equivalent to the European Economic Area (EEA). The CJEU did not answer this question in its judgment of 6 October 2015, but noted concerns regarding reports of indiscriminate mass surveillance by the National Security Agency (NSA)[1] and the Federal Bureau of Investigation (FBI) in the United States. Since then, the EU Commission and the U.S. Department of Commerce agreed on a new "EU-U.S. Privacy Shield Program," which is accompanied by assurances by a number of U.S. government authorities regarding privacy protections relating to surveillance programs.[2]

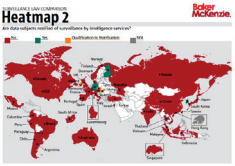
At the same time, other institutions in the EU and scholars started to analyze the state of surveillance laws in individual jurisdictions within the EEA and elsewhere. They uniformly found comparisons difficult, as actual practices of intelligence authorities are cloaked in secrecy

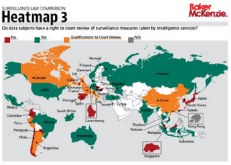
[1] CJEU C-362/14 Schrems v. Data Protection Commissioner), 6.10.2015, #31.
[2] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

and laws are complex and fragmented in this area.[3] Due to constitutional limitations on the EU's jurisdiction to legislate matters of national security, the legal situation in the EEA member states is not very uniform. For example, in some EEA member states, senior police or military officers can issue search warrants.[4] EU institutions have called for improvements in the U.S. as well as in the EEA.[5]

Companies around the world are confronted with questions on how to comply with different jurisdictions' laws and data access requests. Users and providers of cloud services, Software-as-a-Service and other services have to factor in government surveillance and data access practices of different countries into their business and location plans. With our surveillance law survey and heat map, we intend to contribute a global overview with broad jurisdictional scope to the discussion and corporate planning processes.

See our heat maps here:

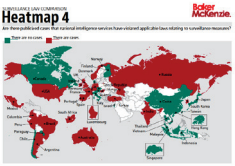


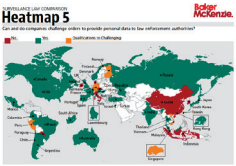


[3] Cate/Dempsey/Rubinstein, Systematic government access to private-sector data, 2 International Data Privacy Law, 215 (2012); Schwartz, Systematic government access to private-sector data in Germany, 2 International Data Privacy Law, 289 (2012); Brown, Government access to private-sector data in the United Kingdom, 2 International Data Privacy Law, 230 (2012). Freiwald/ Métille, Reforming Surveillance Law: the Swiss Model, 28 Berkeley Tech. L. J., 1261 (2013).

[4] See Study of the EU Agency for Fundamental Rights (FRA), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks (2015), http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services": A comparison between US and EU data protection legislation for law enforcement purposes, www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf.

[5] See studies cited in footnote 38





Of course, the situation regarding individual data access requests and responses is more nuanced than a comparative overview survey can address. Therefore, companies cannot rely on our overview as legal advice regarding a particular situation and have to continue to assess their own individual situation based on the pertinent facts and circumstances. Please contact us with any questions or suggestions.

Baker McKenzie's Global Data Security Leadership Team

Brian Hengesbaugh (Chicago)
+1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Lothar Determann (Palo Alto)
+1 650 856 5533
lothar.determann@bakermckenzie.com

Patrick Fair (Sydney)
+61 2 8922 5534
patrick.fair@bakermckenzie.com

Paul Forbes (Sydney)
+61 2 8922 5346
paul.forbes@bakermckenzie.com

Francesca Gaudino (Milan)
+39 02 76231 452
francesca.gaudino@bakermckenzie.com

Theo Ling (Toronto)
+1 416 865 6954
theo.ling@bakermckenzie.com

Carolina Pardo (Bogota)
+571 634 1559
carolina.pardo@bakermckenzie.com

Michael Stoker (Chicago)
+1 312 861 2870
michael.stoker@bakermckenzie.com

Contributing Lawyers

Argentina

Guillermo Cervio
Buenos Aires
Tel: +54 11 4310 2223
guillermo.cervio
@bakermckenzie.com

Roberto Grané
Buenos Aires
Tel: +54 11 4310 2214
roberto.grane
@bakermckenzie.com

Australia

Patrick Fair
Sydney
Tel: +61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Sydney
Tel: +61 2 8922 5204
adrian.lawrence
@bakermckenzie.com

Ju Young Lee
Sydney
Tel: +61 2 8922 5260
juyoung.lee@bakermckenzie.com

Austria

Lukas Feiler
Vienna
Tel: +43 1 24250 450
lukas.feiler@bakermckenzie.com

Marisa Schlacher
Vienna
Tel.: +43 1 2 42 50 278
marisa.schlacher
@bakermckenzie.com

Brazil

Flavia Rebello
Sao Paulo
Tel: +55 11 3048 6851
flavia.rebello@trenchrossi.com

Gabriela Paiva-Morette
Sao Paulo
Tel: +55 11 3048 6785
gabriela.paiva-morette
@trenchrossi.com

Canada

Theodore Ling
Toronto
Tel: +416 865 6954
theodore.ling
@bakermckenzie.com

Jonathan Tam
Toronto
Tel: +416 865 2324
jonathan.tam
@bakermckenzie.com

Chile

Diego Ferrada
Santiago
Tel: +56 22 367 7087
diego.ferrada
@bakermckenzie.com

Antonio Ortuzar, Jr.
Santiago

Tel: +56 22 367 7078
antonio.ortuzar.jr
@bakermckenzie.com

China (PRC)

Howard Wu
Shanghai
Tel: +86 21 6105 8538
howard.wu@bakermckenzie.com

Chris Jiang
Shanghai
Tel: +86 21 6105 5910
chris.jiang@bakermckenzie.com

Colombia

Carolina Pardo
Bogota
Tel: +57 1 634 1559
carolina.pardo
@bakermckenzie.com

Sandra Castillo
Bogota
Tel: +57 1 634 1530
sandra.castillo
@bakermckenzie.com

Daniela Cala
Bogota
Tel: +57 1 634 1500
daniela.cala
@bakermckenzie.com

Czech Republic

Jiri Cermak
Prague
Tel: +420 236 045 001
jiri.cermak@bakermckenzie.com

Milena Hoffmanova
Prague
Tel: +420 236 045 001
milena.hoffmanova
@bakermckenzie.com

Denmark

Tina Brøgger Sørensen
Copenhagen
Tel: +45 38 77 44 08
tib@kromannreumert.com

Daiga Grunte-Sonne
Copenhagen
Tel: +45 38 77 41 18
DSO@kromannreumert.com

Finland

Samuli Simojoki
Helsinki
Tel: +358 20 713 3500
mobile +358 40 571 3303
samuli.simojoki@borenius.com

Susanna Niittymaa
Helsinki
Tel: + 358 20 713 3298
susanna.niittymaa@borenius.com

France

Denise Lebeau-Marianna
Paris
Tel: +33 1 44 17 53 33
denise.lebeau-marianna
@bakermckenzie.com

Magalie Dansac Le Clerc
Paris
Tel: +33 1 44 17 59 82
magalie.dansacleclerc
@bakermckenzie.com

Hugo Roy
Paris
Tel: +33144176560
hugo.roy@bakermckenzie.com

Germany

Joachim Scherer
Frankfurt
Tel: +49 69 2 99 08 189
joachim.scherer
@bakermckenzie.com

Caroline Heinickel
Frankfurt
Tel: +49 69 2 99 08 416
caroline.heinickel
@bakermckenzie.com

Andreas Neumann
Frankfurt
Tel: +49 69 2 99 08 310
caroline.heinickel
@bakermckenzie.com

Hong Kong

Paolo Sbuttoni
Hong Kong
Tel: +852 2846 1521
paolo.sbuttoni
@bakermckenzie.com

Gillian Lam
Hong Kong
Tel: +852 2846 1686
gillian.lam@bakermckenzie.com

Hungary

Ines K. Radmilovic
Budapest
Tel: +36 1 302 3330
ines.radmilovic
@bakermckenzie.com

Adam Liber
Budapest
Tel: +36 1 302 3330
adam.liber@bakermckenzie.com

Janos Puskas
Budapest
Tel: +36 1 302 3330
janos.puskas
@bakermckenzie.com

India

Probir Roy Chowdhury
Bangalore
Tel: +91-80-43503618
probir@jsalaw.com

Sajai Singh
Bangalore
Tel: +91-98450 78666
sajai@jsalaw.com

Indonesia

Hendronoto Soesabdo
Jakarta
+62 21 2960 8610
hendronoto.soesabdo
@bakernet.com

Reno Hirdarisvita
Jakarta
Tel: +62 21 2960 8571
reno.hirdarisvita@bakernet.com

Ireland

John Cahir
Dublin
Tel: +353 1 649 2943
jcahir@algoodbody.com

Alison Quinn
Dublin
Tel: +353 1 649 2461
alquinn@algoodbody.com

Israel

Nurit Dagan
Tel Aviv
Tel: +972 3 692 7424
dagan@hfn.co.il

Daniel Reisner
Tel Aviv
Tel: +972 3 692 2884
reisnerd@hfn.co.il

Italy

Francesca Gaudino
Milan
Tel: +39 02 76231 452
francesca.gaudino
@bakermckenzie.com

Japan

Daisuke Tatsuno
Tokyo
Tel: +813 6271 9479
daisuke.tatsuno
@bakermckenzie.com

Kensaku Takase
Tokyo
Tel: +813 6271 9752
kensaku.takase
@bakermckenzie.com

Luxembourg

Laurent Fessmann
Luxembourg
Tel: +352 261844 205
laurent.fessmann
@bakermckenzie.com

Amaury-Maxence Bagot
Luxembourg
Tel: +352 261844 288
salome.steinberger
@bakermckenzie.com

Malaysia

Woo Wei Kwang
Kuala Lumpur
Tel: +603 2298 7898
weikwang.woo
@wongpartners.com

Shameen Binti Mohd. Haaziq Pillay
Kuala Lumpur
Tel: +603 2298 7943
shameen.mohd.haaziqpillay
@wongpartners.com

Mexico

Sergio Legorreta-Gonzalez
Mexico City
Tel: +52 55 5279 2954
sergio.legorreta-
gonzalez@bakermckenzie.com

Carlos Vela-Trevino
Mexico City
Tel: +52 55 5279 2911
carlos.vela-trevino@bakermckenzie.com

Norway

Espen Sandvik
Oslo
Tel: +47 98 29 45 41
esa@adeb.no

Paraguay

Nestor Loizaga
Asuncion
Tel: +595 21 318 3117
nloizaga@ferrere.com

Raul Pereira
Asuncion
rapereira@ferrere.com

Peru

Teresa Tovar
Lima
Tel: +51 1 618 8500 Ext. 552
teresa.tovar@bakermckenzie.com

Viviana Chavez
Lima
Tel: +51 1 618 8500 Ext. 421
viviana.chavez@bakermckenzie.com

Portugal

César Bessa Monteiro
Lisbon
Tel: +351 213 264 747
cesar.bmonteiro@pbbr.pt

César Bessa Monteiro, Jr.
Lisbon
Tel: +351 213 264 747
c.monteiro@pbbr.pt

Ricardo Henriques
Lisbon
Tel: +351 213 264 747
ricardo.henriques@pbbr.pt

Russia

Edward Bekeschenko
Moscow
Tel: +7 495 787 2700
ed.bekeschenko@bakermckenzie.com

Evgeny Reyzman
Moscow
Tel: +7 495 787 2700
evgeny.reyzman@bakermckenzie.com

Vadim Perevalov
Moscow
Tel: +7 495 787 2700
vadim.perevalov@bakermckenzie.com

Alexander Monin
Moscow
Tel: +7 495 787 2700
alexander.monin@bakermckenzie.com

Roman Butenko
Moscow
Tel: +7 727 330 0500
roman.butenko
@bakermckenzie.com

Oleg Blinov
Moscow
Tel: +7 495 787 2700
oleg.blinov@bakermckenzie.com

Oleg Tkachenko
Moscow
Tel: +7 495 787 2700
oleg.tkachenko
@bakermckenzie.com

Singapore

Ken Chia
Singapore
Tel: +65 6434 2558
ken.chia@bakermckenzie.com

South Africa

Darryl Bernstein
Johannesburg
Tel: +27 0 11 911 4367
darryl.bernstein
@bakermckenzie.com

Widaad Ebrahim
Johannesburg
Tel: +27 0 11 911 4384
widaad.ebrahim
@bakermckenzie.com

Deepa Ramjee
Johannesburg
Tel: +27 0 11 911 4368
deepa.ramjee
@bakermckenzie.com

South Korea

Boseong Kim
Seoul
Tel: +82 2 721 4130
boskim@kcllaw.com

Junghwa Lee
Seoul Tel: +82 2 721 4147
jhlee@kcllaw.com

Mike Shin
Seoul
Tel: +82 2 721 4140
mikeshin@kcllaw.com

Spain

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com

Ignacio Vela
Madrid
Phone: +34 91 230 45 09
ignacio.vela@bakermckenzie.com

Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang
@bakermckenzie.com

Tehsin Wu
Taipei

Tel: +886 2 2715 7327
tehsin.wu@bakermckenzie.com

Thailand

Dhiraphol Suwanprateep
Bangkok
Tel: +66 02 636 2000 Ext. 4950
dhiraphol.suwanprateep
@bakermckenzie.com

Pattaraphan Paiboon
Bangkok
Tel: +66 02 636 2000 Ext. 4568
pattaraphan.paiboon
@bakermckenzie.com

Turkey

Hakki Can Yildiz
Istanbul
Tel: +90 212 376 64 54
can.yildiz@esin.av.tr

Can Sozer
Istanbul
Tel: +90 212 376 64 43
can.sozer@esin.av.tr

Hilal Temel
Istanbul
Tel: +90 212 376 64 17
hilal.temel@esin.av.tr

United Kingdom

Ian Walden
London
Tel: +44 207 9191 247
ian.walden@bakermckenzie.com

Dyan Heward-Mills
London
Tel: +44 207 9191 269
dyann.heward-
mills@bakermckenzie.com

United States

Lothar Determann
Palo Alto
Tel: +1 650 856 5533
lothar.determann
@bakermckenzie.com

Brian Hengesbaugh
Chicago
Tel: +1 312 861 3077
brian.hengesbaugh
@bakermckenzie.com

Michael Mensik
Chicago
Tel: +1 312 861-8941
michael.mensik
@bakermckenzie.com

Michael Egan
Washington, D.C.
Tel: +1 202 452 7022
michael.egan
@bakermckenzie.com

Vietnam

Yee Chung Seck
Ho Chi Minh City
Tel: +84 8 829 6234
yeechung.seck
@bakermckenzie.com

Chi Anh Tran
Ho Chi Minh City
Tel: +84 8 3520 2625
chianh.tran@bakermckenzie.com

*This list includes just some of our global Data Security practitioners. To find a Baker McKenzie lawyer or other professional, please visit www.bakermckenzie.com.

Table of Contents

Argentina

Guillermo Cervio
Buenos Aires
Tel: +54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Roberto Grané
Buenos Aires
Tel: +54 11 4310 2214
roberto.grane@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

4. How can intelligence services compel companies to provide access to data?

Through court orders.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Possibly, yes. One of the purposes of the Federal Intelligence Agency is to strengthen relations with intelligence agencies from other countries.

6. Are data subjects notified of surveillance by intelligence services?

Generally, no.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Data subjects have the right to file reports with the Bicameral Commission of Intelligence Institutions and Activities when the Federal Intelligence Agency has committed abusive or illicit actions.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes. To the best of our knowledge, the Judicial Control Department and the Bicameral Commission of Intelligence Institutions and Activities are notified of surveillance measures undertaken by intelligence services.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

The Judicial Control Department needs to be notified ex ante. We are not aware of any right to object. The Bicameral Commission of Intelligence Institutions and Activities is notified of the surveillance measures ex post, during the annual inspection of intelligence activities.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes. In 2015, a judicial case was filed by two national deputies, reporting the existence of an illegal spying system carried out by the Federal Intelligence Agency on judges, politicians, journalists and businessmen, which gained some media attention. The case is still ongoing.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Companies can be compelled to provide access to data via warrants for live interception and location information and court orders for stored communications.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Under local privacy regulations, data subjects have the right to request for access, rectification, update and/or elimination of their personal data from any database (either private or public). Data subjects can also file judicial claims for damages or criminal penalties. In case of intelligence-related activities, data subjects can also file reports with the Bicameral Commission of Intelligence Institutions and Activities.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable to Argentina.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Generally, yes. Nevertheless, there have not been any significant high profile cases in which data subjects have reported illegal transfers of data of companies to the government.

17. Are data subjects notified if law enforcement accesses their data?

Generally, no. For national security reasons, intelligence investigations are often conducted on a confidentiality basis.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Australia

Patrick Fair
Sydney
Tel: +61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Sydney
Tel: +61 2 8922 5204
adrian.lawrence@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes, warrants are required to access content of messages in transit and in storage. Access to metadata relating to use of communications services does not require a warrant.

4. How can intelligence services compel companies to provide access to data?

Court orders are required for access to the content of messages. A nominated collection of national security, law enforcement and police integrity agencies have power to issue notices requiring data without the issue of a warrant. Some state agencies have independent evidence collection powers that can apply to data but operate outside the federal law.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, Australian intelligence services cooperate and exchange information with the Five Eyes Alliance and others. Australia is a participant in the Mutual Assistance in Criminal matters community of nations.

6. Are data subjects notified of surveillance by intelligence services?

No. It is an offence for a communications services provider to disclose information regarding the issue of a surveillance warrant and/or the issue of a request for metadata.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes, but subject to the discretion of the Inspector-General (the statutory authority who can investigate actions of the Australian intelligence and security agencies).

Metadata collected under the mandatory data retention regime requires that a specified set of metadata be collected by ISPs, carriers and carriage service providers. Account and service information must be held for two years from when the account is closed. Other information must be held for two years from collection. This information is subject to the Privacy Act and can be accessed and corrected by the data subject, but the data subject is not entitled, under that law, to find out if it has been accessed or used.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes, in certain cases, ministers and the attorney general are notified of individual surveillance measures via the warrant request process, and intelligence/ security parliamentary committees are notified when surveillance agency heads give certain directions. There is a public interest advocate who has a role in decision-making related to accessing metadata relating to the communications of a journalist. The metadata retention scheme is subject to review and reporting by the Commonwealth Ombudsman.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

For notification via warrants, the notification is prior to the surveillance occurring. The relevant minister or parliamentary committee can raise an inquiry with the Inspector-General.

For notification of directions, the notification occurs after the direction has been made.

Notifications for access to metadata are complied with under a general measure requiring telecommunications companies ("telcos") to assist law enforcement. This provision does allow some scope for telcos to test the legitimacy of requests in limited cases.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

The Snowden leaks identified that Australia has been actively monitoring mobile phones of the Indonesian leadership and that Australia bugged offices in East Timor to win the upper hand in resource access negotiations.

11. Do law enforcement authorities need court orders to intercept communications?

Yes, subject to exceptions e.g., emergencies, the consent of the parties.

12. How can law enforcement authorities compel companies to provide access to data?

Companies can be compelled to provide access to data via warrants under telecommunications legislation including for interception of live and stored communications and in relation to metadata, by using a

notice issued on a telco, ISP or carriage service provider. State Authorities, in some cases, have independent information gathering powers that can be used to obtain information held by telcos.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

Companies will usually reject law enforcement requests from an agency if it is invalid or if the information could be obtained through different processes.

Large telecommunications companies such as Telstra and Optus expressly state in their privacy policies that they will reject any request for personal information that does not comply with legal requirements.

Note that telcos are paid for delivery of data to law enforcement authorities and have systems for providing information on a regular basis for payment.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

There are no constitutional protections in Australia.

Against Companies: Individuals can complain to the privacy regulator who has the power to investigate, seek determinations and enforceable undertakings and apply for court enforced penalties.

Against Government: Provided that the information is shared under the exceptions in the Privacy Act, no privacy rights other than those required generally with respect to the collection, holding etc. of personal information.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

No. There is no reciprocal Privacy Shield program between Australia and the EU as exists between the U.S. and EU.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Telcos are immune from liability in instances where they render assistance to law enforcement or national security agencies and provided that they act in good faith. However, telcos may be liable to data subjects for breaching the Privacy Act if they do not take reasonable steps to protect personal information from unauthorized access or disclosure.

17. Are data subjects notified if law enforcement accesses their data?

No.

Companies are not permitted by law to notify customers if individual agencies have made a request for customer information.

Government is generally not under an obligation to notify individuals if they access their data.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 requires telecommunications companies to retain metadata about customers for 2 years. This includes information such as contact information of the individual, the time of call, the location of the equipment, who they called, where they called,

the duration of the call, the medium but not the actual content of message or phone call. This will significantly increase the amount of data retained on individuals. The government has recently invited submissions on whether to expand the degree to which this data may be accessed for use in civil proceedings.

Austria

Lukas Feiler
Vienna
Tel: +43 1 24250 450
lukas.feiler@bakermckenzie.com

Marisa Schlacher
Vienna
Tel.: +43 1 2 42 50 278
marisa.schlacher@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

No, there are no blanket surveillance programs that exist in Austria (either disclosed publicly or likely to exist in secret).

2. Are intelligence services authorized to conduct surveillance for an economic purpose

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Not applicable (there is no possibility for intelligence services to intercept calls, emails, or other communications).

4. How can intelligence services compel companies to provide access to data?

Not applicable (there is no possibility for intelligence services to compel companies to provide access to data).

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes, if they learn that they have been the subject of targeted surveillance.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes, an Ombudsman has to be notified.

As regards foreign surveillance measures, the Ministry of National Defense has to be notified.

In all other cases, the Ministry of the Interior has to be notified.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

The Ombudsman is notified ex ante.

The Ministries of the Interior and of National Defense are typically notified ex post. The relevant ministry has the authority to instruct national intelligence services at any time and, thus, also the right to object to the measures.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

A public prosecutor may order the seizure of data without a court order (§111 Criminal Procedure Code).

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

Companies may file a complaint with the criminal court of first instance against a data seizure ordered by a public prosecutor (§106 Criminal Procedure Code), demanding legal review of the seizure.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against government agencies: Filing a complaint against the agency either in criminal court or in administrative court, demanding legal review of the seizure; in case of public authorities other than law enforcement authorities, initiating a proceeding before the Data Protection Authority, demanding deletion of the data.

Against companies: Filing a civil lawsuit demanding deletion of the data; seeking a permanent and/or preliminary injunction.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Against U.S. companies: Yes, if (1) the U.S. company has an establishment in Austria and processes the data in the context of the activities of that establishment or (2) the U.S. company has no establishment in the EU but processes the data in Austria.

Against the U.S. government: The U.S. government is subject to sovereign immunity. Therefore, no claims may be brought against it.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes.

If companies disclose personal data without sufficient legal basis, criminal penalties may apply (depending on applicable sector-specific regulation) and civil liability claims might be brought against the company in case the disclosure of data results in the public exposure of private facts. Furthermore, the Data Protection Act 2000 provides administrative penalties in the amount of up to EUR 25,000.

17. Are data subjects notified if law enforcement accesses their data?

Generally, yes.

Data subjects have to be notified in case they have been the subject of lawful interception (§138(5) Criminal Procedure Code). They also have to be notified in case telecommunication traffic or location data is disclosed to law enforcement agencies.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Brazil

Flavia Rebello
Sao Paulo
Tel: +55 11 3048 6851
Flavia.Rebello@trenchrossi.com

Gabriela Paiva-Morette
Sao Paulo
Tel: +55 11 3048 6785
gabriela.paiva-morette@trenchrossi.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Not applicable.

The Brazilian Intelligence Agency ("ABIN") is not authorized to intercept calls, e-mail or other communications. Such interceptions may be executed only by the police authority or the District Attorney, upon court order.

4. How can intelligence services compel companies to provide access to data?

ABIN is not competent to compel companies to provide access to data. Nevertheless, competent authorities need court orders to be granted access to data.

5. Are national intelligence services cooperating and exchanging information with foreign services?

ABIN may execute cooperation agreements if there is convergence of national interests with other countries and the President deems it appropriate.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

In theory, yes. If surveillance measures affect individual rights and guarantees established in the Federal Constitution or in the Civil Code, the individual should have the right to court review of surveillance measures.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No. However, ABIN may cooperate with other federal governmental bodies that form part of the Brazilian Intelligence System.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes. There was a discussion in 2008 concerning ABIN's actions in the course of Operation Satiagraha (which investigated the misuse of public funds, corruption and money laundering). It was revealed, during the Operation, that ABIN participated in criminal investigations and therefore certain evidence used against the suspects were found null and void.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Through court orders.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Companies can challenge orders to provide personal data to law enforcement authorities mainly if such order is not grounded on applicable law. Nevertheless, it is common for such court orders to determine a (usually high) daily fine for companies that fail to comply. Also, failure to comply with court orders may be deemed a crime under local laws, so challenging any such court order is not without risk.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Personal data in Brazil is protected by general principles contained in the Federal Constitution, Civil Code and also in the Internet Legal Framework.

Accordingly, an individual's right to intimacy, privacy, honor and image is considered a fundamental right subject to protection under the Brazilian Federal Constitution. Likewise, the Federal Constitution grants special protection to the secrecy of correspondence, telegraphic, data and telephone communications. Furthermore, the Brazilian Civil Code treats the right to privacy as a personality right, which cannot be waived or assigned as a matter of public policy. The Internet Legal Framework stresses Internet users' right to privacy

online. As a result of such laws, sharing personal data without the data subject's consent or the relevant court order may give rise to penalties and claims for damages and/or injunctions.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Generally, yes. The general rule is that disclosure of personal data is only permitted with the data subject's consent or under a relevant court order.

17. Are data subjects notified if law enforcement accesses their data?

Generally, no.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Canada

Theodore Ling
Toronto
Tel: +416 865 6954
theodore.ling@bakermckenzie.com

Jonathan Tam
Toronto
Tel: +416 865 2324
jonathan.tam@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

4. How can intelligence services compel companies to provide access to data?

Companies can be compelled to provide access to data through court orders or warrants issued by the courts.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, cooperation with foreign governments and intelligence services is contemplated by legislation.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Although there is no general statutory right to seek judicial review of surveillance measures taken by intelligence services, if a data subject were to independently discover that he or she were subject to

surveillance by the intelligence services, he or she could challenge the constitutionality or legality of such measures in court.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No, it does not appear that the intelligence service is legally required to notify other governmental bodies of individual surveillance measures to be undertaken.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No, not to date.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Law enforcement authorities can compel companies to provide access to data through court orders or warrants issued by the courts.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

A company may challenge, by court process, an order to provide personal data based on the legal and factual grounds upon which the order was made. Objection may also be raised by invoking privacy considerations protected under Canadian constitutional law or privacy legislation, such as the federal Personal Information Protection and Electronic Documents Act. A company may also challenge whether any national security exceptions to the non-disclosure of such data have been satisfied.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Individuals generally hold privacy rights that prohibit companies from disclosing their personal information to the government. However, those privacy rights, as well as any right to bring suit against the government, may be subject to national security and other exceptions, depending on the right and the alleged breach, in applicable legislation.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes.

A data subject may bring civil suit, or file a complaint with the Privacy Commissioner of Canada for infringement of the Personal Information Protection and Electronic Documents Act, if a company wrongfully discloses personal information. On hearing of the complaint, an award of damages or order for compliance may be made against the company. Similar remedies exist under certain provincial privacy laws.

17. Are data subjects notified if law enforcement accesses their data?

No, data subjects are not usually notified if law enforcement legally accesses their data, unless criminal charges are subsequently brought and disclosure then made as part of the court process.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Government of Canada institutions are statutorily authorized to disclose, with immunity from civil suit, information regarding “activities that undermine the security of Canada” with other federal government institutions, including the Canadian Security Intelligence Service.

Further, a company or non-government organization may voluntarily disclose personal information to a government agency where the organization suspects that the information relates to national security.

Chile

Diego Ferrada
Santiago
Tel: +56 22 367 7087
diego.ferrada@bakermckenzie.com

Antonio Ortuzar, Jr.
Santiago
Tel: +56 22 367 7078
antonio.ortuzar.jr@bakermckenzie.com

1. **Do intelligence services operate surveillance programs to protect national security?**

No.

2. **Are intelligence services authorized to conduct surveillance for an economic purpose?**

No.

3. **Do intelligence services need court orders to intercept calls, emails or other communications?**

Yes.

4. **How can intelligence services compel companies to provide access to data?**

There is no clear way to do this.

5. **Are national intelligence services cooperating and exchanging information with foreign services?**

Probably yes, but informally.

6. **Are data subjects notified of surveillance by intelligence services?**

No.

7. **Do data subjects have a right to court review of surveillance measures taken by intelligence services?**

No, at least not clearly.

8. **Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of**

(individual) surveillance measures taken by intelligence services?

No.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

They need to obtain a court order.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes. There is no significant case law on the subject.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Habeas Data.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes. There is no significant case law on the subject.

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

The Chilean intelligence agency is very small and under funded. They do not have significant financing to conduct a serious surveillance program.

China

Howard Wu
Shanghai
Tel: +86 21 6105 8538
howard.wu@bakermckenzie.com

Chris Jiang
Shanghai
Tel: +86 21 6105 5910
chris.jiang@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose

Under the National Security Law of China, economic security is considered basis of national security. Intelligence services are authorized to collect intelligence that relates to national security, which should include intelligence that relates to economic security. However, there is no specific authorization to conduct industrial espionage or further national economic interests.

Neither is there such specific authorization under the new Cybersecurity Law of China (to take effect from June 1, 2017), which aims to promote a sound development of economic and social informatization and allows intelligence services' intelligence collection for national security and criminal investigation purposes.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

No.

4. How can intelligence services compel companies to provide access to data?

Under the National Security Law of China, citizens and organizations have a legal obligation to cooperate with the investigations of intelligence services for national security purposes and provide information as requested.

By producing his Investigator ID Card, a member of the intelligence services can demand cooperation by citizens and organizations.

Similarly, under the Cybersecurity Law of China, all network operators are obliged to provide technical support and assistance to the intelligence services in the course of national security safeguarding and criminal offenses investigation activities.

5. Are national intelligence services cooperating and exchanging information with foreign services?

The National Security Law of China confirms the need for exchange and cooperation with foreign governments and international organizations.

The Cybersecurity Law of China also indicates a trend of more active international exchange and cooperation in terms of cyberspace governance and suppression of criminal offenses in cyberspace, etc.

Information about actual exchange / cooperation with foreign services (if any) is not in the public domain.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Legally, yes, under the National Security Law of China, citizens and organizations have the right to put forward complaints and charges against the violation of law and neglect of duty in the state security work of the state organs and their staff.

However, we are not aware of any publicized cases.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of

(individual) surveillance measures taken by intelligence services?

There is no specific requirement under the National Security Law or the Cybersecurity Law of China to notify governmental bodies of surveillance measures.

Whether a higher level of government body is notified of such measures in practice, is not publicly known.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

There are no publicized cases in China.

11. Do law enforcement authorities need court orders to intercept communications?

Assuming "law enforcement authorities" refer to the Public Security Bureau and the National Security Bureau in the context of criminal investigations (same below), no.

12. How can law enforcement authorities compel companies to provide access to data?

Law enforcement authorities can compel companies to provide access to data by furnishing supporting documents issued by the people's Procuratorate or the Public Security Bureau.

As mentioned above, under the Cybersecurity Law of China, all network operators are obliged to provide technical support and assistance to the Public Security Bureau and the National Security

Bureau in the course of national security safeguarding and criminal offenses investigation activities.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

In the context of a criminal investigation, no. Under the Criminal Procedural Law, the court, the Procuratorate and the Public Security Bureau have the right to collect evidence; individuals and organizations have the obligation to provide evidence.

Theoretically, companies subject to such orders may file an administrative litigation with the court with competent jurisdiction, or file an administrative appeal/reexamination request with the supervising government authority of the law enforcement authorities, if such orders could be deemed as administrative in nature and have allegedly jeopardized such companies' legitimate rights and interests. However, we are not aware of any publicized cases. Furthermore, in principle, the initiation of such administrative appeal or litigation procedures cannot stop the enforcement of such administrative orders.

However, the law provides that to the extent information concerning personal privacy is collected by law enforcement authorities as evidence in the course of due performance of their duties, such evidence shall be kept confidential. Investigators are also required to keep confidential personal information that comes to their knowledge in the course of an investigation.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Government agencies and individual investigators have a duty to preserve the confidentiality of personal information that is disclosed to them in the law enforcement process.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Assuming that the question is whether a foreigner can assert privacy rights against a Chinese company and the Chinese government.

Yes, to the extent privacy rights are protected under PRC laws.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Probably no, if the data is provided according to government request.

Disclosure of personal data to the government is not considered a leakage of personal data, and is generally not objectionable. Liability may arise if personal data is divulged to third parties which causes damage to the data subject.

17. Are data subjects notified if law enforcement accesses their data?

Generally, no.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

The operation and working procedures of intelligence services in this country are top secret. There is virtually no public information of how they function, and as a matter of reality, their work is generally outside of judicial review.

Colombia

Carolina Pardo
Bogota
Tel: +57 1 634 1559
carolina.pardo@bakermckenzie.com

Sandra Castillo
Bogota
Tel: +57 1 634 1530
sandra.castillo@bakermckenzie.com

Daniela Cala
Bogota
Tel: +57 1 634 1500
daniela.cala@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose

No

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes

4. How can intelligence services compel companies to provide access to data?

Through court orders. However the Law provides as an alternative the subscription of inter-institutional agreements between intelligence services and private entities through which the latter can supply information to the former.

5. Are national intelligence services cooperating and exchanging information with foreign services?

We do not have information regarding actual cooperation and exchange of information with foreign services.

However, Colombian Law does accept the possibility for Colombian intelligence agencies to cooperate with foreign intelligence agencies. For instance there have been at least two intents to establish cooperation agreements between Colombia and the United States and Colombia and the NATO countries. However, such agreements were declared as contrary to the Colombian Constitution by the Constitutional Court.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

The Intelligence and Counterintelligence Law (Law 1621 of 2013) does not establish a mechanism through which data subjects may exercise a right to court review of surveillance measures taken by intelligence services.

Nevertheless, any measure or activity taken by intelligence services must be authorized in an Operation Order or in a Work Mission, that may be issued by the directors of the entities or the chiefs or deputy chiefs of the units, sections or dependencies within each organization.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes. The police inspectors or the Military Forces to which intelligence services that take intelligence measures are part, must present an annual report before the Ministry of Defense and the Legal Commission for the Monitoring of Intelligence and Counterintelligence Measures. The latter is a Congress Committee created by the Intelligence and Counterintelligence Law (Law 1621 of 2013).

Additionally, the Legal Commission for the Monitoring of Intelligence and Counterintelligence Measures presents a report addressed to the President regarding the compliance of the intelligence measures with applicable laws.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

They are notified ex post and do not have the right to object the measures.

The authorization of the intelligence measures is granted by the directors of the entities or the chiefs or deputy chiefs of the units, sections or dependencies within each organization. Therefore they may be able to object the measures.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes, there is one major case in which the national intelligence services violated applicable laws relating to surveillance measures.

The former Colombian intelligence agency, known as the Administrative Department of Security (DAS), intercepted calls and performed illegal monitoring to leaders of the opposition, judicial agents, journalists and State agents.

This had as a consequence the elimination of the DAS and the creation of a new agency known as the National Direction of Intelligence (DNI). Additionally, some individuals with high-ranked positions within the organization and the government were condemned.

11. Do law enforcement authorities need court orders to intercept communications?

Yes

12. How can law enforcement authorities compel companies to provide access to data?

Court orders, subpoenas and exhibition orders issued by a judicial authority

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes. For instance when the enforcement authority requests personal data outside its legal mandate.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Data subjects have the following rights:

- Know, update and correct their Personal Data
- Request proof of the consent granted to the company to collect an process their Personal Data, have access to their Personal Data and, in general, be informed about the uses that their Personal Data is been subject to.
- Revoke the authorization granted to the company and/or request the elimination of their Personal Data when they consider there is a violation to the principles, rights and constitutional and legal guarantees.
- Access the Personal Data that was collected and processed.
- Present a complaint or claim before the Data Protection Officer of the Company.
- If the Data Protection Officer does not attend said complain, have recourse to the Superintendence of Industry and Commerce and present their queries, complaints or claims.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

If companies disclose data to governmental authorities in the exercise of their legal functions or they disclose data due to a judicial order, then no.

If companies disclose data to governmental authorities outside the exercise of their legal functions, then yes.

17. Are data subjects notified if law enforcement accesses their data?

Usually not.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Czech Republic

Jiri Cermak
Prague
Tel: +420 236 045 001
jiri.cermak@bakermckenzie.com

Milena Hoffmanova
Prague
Tel: +420 236 045 001
milena.hoffmanova@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose

Yes, in theory, intelligence services may be authorized to conduct industrial espionage should it be necessary for protection of the state, significant economic interests, security and defense of the Czech Republic.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes, in general, intelligence services need specific court orders for breach of individuals' privacy rights.

4. How can intelligence services compel companies to provide access to data?

Through court orders.

5. Are national intelligence services cooperating and exchanging information with foreign services?

This is not publicly available information.

6. Are data subjects notified of surveillance by intelligence services?

Data subjects are supposed to be generally notified ex post. However, in practice, only a small percentage of data subjects is notified.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

No.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Not on an individual basis, however, they may request details of activities of intelligence services at any point. The governmental bodies with such power include the government and the president.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Usually ex post. There is no subjective right of the governmental bodies to object. However, if the criminal authorities learn about a breach of legal regulation, they may start legal proceedings against responsible persons within the intelligence agencies.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No, we are not aware of any publicized cases.

11. Do law enforcement authorities need court orders to intercept communications?

Yes. However, a court order is not necessary for certain criminal offences (e.g., trafficking, restriction of personal freedom) if the user of the intercepted station agrees.

12. How can law enforcement authorities compel companies to provide access to data?

Depending on the type of data, however, usually using court orders.

It depends on the type of data involved. Usually, court orders are necessary for law enforcement authorities to compel companies to provide access to data.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

No.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

No, provided the data is shared on valid legal grounds. If not, the sharing can be challenged in both civil as well as criminal proceedings. Data subjects may seek damages or injunctions.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Yes, based on European Commission approved contractual clauses, i.e., on the contractual basis, or Privacy Shield system.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes, however, there is no public record of any significant case.

17. Are data subjects notified if law enforcement accesses their data?

Data subjects are supposed to be generally notified ex post. However, in practice, only a small percentage of data subjects is notified.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

As this area is quite sensitive, there is no sufficient information available on public record.

Denmark

Tina Brøgger Sørensen
Copenhagen
Tel: +45 38 77 44 08
tib@kromannreumert.com

Daiga Grunte-Sonne
Copenhagen
Tel: +45 38 77 41 18
DSO@kromannreumert.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes, by virtue of cf. section 72 of the Danish Constitution.

4. How can intelligence services compel companies to provide access to data?

During investigation:

Seizures, cf. the rules in the Danish Administration of Justice Act (requires a court order)

Order to present documents with relevance to the investigation, cf. the Danish Administration of Justice Act, section 804 (requires a court order)

During court cases: Rules on discovery (in Danish: edition)

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes. For instance, The Danish Security and Intelligence Service (in Danish: Politiets Efterretningstjeneste) cooperates and exchanges information with foreign intelligence services on a bilateral level. Multilaterally, the Danish Security and Intelligence Service participates in the European countries' Counter Terrorism Group (CTG).

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes. The Danish Constitution provides for a general right to court review of actions taken by the public authorities, cf. section 63.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Not as a starting point. However, the Danish Security and Intelligence Service has a general duty to notify the Ministry of Justice, and the Danish Defence Intelligence Service (in Danish: Forsvarets Efterretningstjeneste) has a corresponding duty in relation to the Ministry of Defence. This does not specifically single out individual surveillance measures.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

Yes by virtue of cf. section 72 of the Danish Constitution.

12. How can law enforcement authorities compel companies to provide access to data?

During investigation:

Seizures, cf. the rules in the Danish Administration of Justice Act (requires a court order)

Order to present documents with relevance to the investigation, cf. the Danish Administration of Justice Act, section 804 (requires a court order)

During court cases: Rules on discovery (in Danish: edition)

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes. For instance, The Danish Security and Intelligence Service (in Danish: Politiets Efterretningstjeneste) cooperates and exchanges information with foreign intelligence services on a bilateral level. Multilaterally, the Danish Security and Intelligence Service participates in the European countries' Counter Terrorism Group (CTG).

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against public authorities: The Danish Constitution, section 72 (judicial order required for breach of secrecy) and section 71 (liberty) as well as the European Convention on Human Rights art. 8 (respect for private life).

Against companies (data controllers): The Danish Act on Processing of Personal Data contains the following privacy rights for individuals (data subjects):

- Right to be given certain information where the controller collects from the data subject (section 28)
- Right to be given certain information where the controller obtains data from others apart from the data subject (section 29)
- Right to be informed upon request if data are being processed about the data subject (section 31)
- Right to object to the processing of data relating to him/her (section 35)
- Right to have data rectified, erased or blocked if the data turn out to be inaccurate or misleading or in any other way processed in violation of law or regulations (section 37,1)
- Right to request the controller to notify the third party to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the rule stated above (section 37,2)
- Right to withdraw consent (section 38)
- Right to object with the effect that the controller may not make the data subject a subject to a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects (section 39)
- The data subject may file a complaint to the appropriate supervisory authority (the Danish Data Protection Agency, in Danish: Datatilsynet) concerning the processing of data relating to him/her (section 40). The Data Protection Agency may then order a data controller to discontinue a processing operation which may not take place under the Act and to rectify, erase or block specific

data undergoing such processing, cf. section 59 of the Act on Processing of Personal Data.

Furthermore, the Danish Liability and Compensations Act contains a general right to claim torts. Case law has granted torts in the event of infringement of the rights set forth in the Act of Processing of Personal on numerous occasions.

The Danish Administration of Justice Act contains general rules on injunction that can be used in relation to violations of the data processing rules.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

According to section 4(3) of the Act on Processing of Personal Data, the rights contained in the Act are binding upon controllers established in a third country (the U.S.), if:

- The processing of data is carried out with the use of equipment situated in Denmark, unless such equipment is used only for the purpose of transmitting data through the territory of the European Community, or
- The collection of data in Denmark takes place for the purpose of processing in a third country

In October 2015, the former U.S.-EU Safe Harbor Program was overturned by the European Court of Justice in the case of Maximilian Schrems v Data Protection Commissioner. However, the U.S.-EU Safe Harbor Agreement is now replaced with the U.S.-EU Privacy Shield Agreement, effective from 1 August 2016.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes. Companies shall compensate any damage caused by the processing of data in violation of the provisions of the Danish Act on Processing of Personal Data (including the rules contained herein on disclosure). This applies unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data, cf. section 69 of the Danish Act on Processing of Personal Data.

17. Are data subjects notified if law enforcement accesses their data?

Yes. If law enforcement collects data from others than the data subjects themselves, the data subjects must be notified of various matters, including the identity of the law enforcement agency and the purpose of gathering the data in question, cf. section 29 of the Act on Processing of Personal Data.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

There is specific legislation that applies to certain areas, for instance, video surveillance is regulated by a specific executive order.

Finland

Samuli Simojoki
Helsinki
Tel: +358 20 713 3500 | mobile +358 40 571 3303
samuli.simojoki@borenius.com

Susanna Niittymaa
Helsinki
Tel: + 358 20 713 3298
susanna.niittymaa@borenius.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes, to a certain extent.

Finnish intelligence services are generally conducted by the Finnish Security Intelligence Service ("Supo"), the Police of Finland and the Finnish Defence Forces. The Supo is an operational security authority whose core functions are counterterrorism, counterintelligence and security work.

The statutory authority and legal means are mainly stipulated under the Finnish Police Act (872/2011 as amended). The statutory duties of the Supo are defined in the Finnish Act on Police Administration (110/1992 as amended). General authority of the Finnish Defence Forces is stipulated under the Finnish Act on the Defence Forces (551/2007 as amended).

2. Are intelligence services authorized to conduct surveillance for an economic purpose

No.

The general precondition for the use of secret methods of gathering intelligence is that this can be assumed to result in gaining information necessary in preventing, detecting or averting the threat of an offence. Secret intelligence gathering may generally be used in detecting the following offences:

a) compromising the sovereignty of Finland;

b) incitement to war;

c) treason, aggravated treason;

d) espionage, aggravated espionage;

e) disclosure of a national secret;

f) unlawful intelligence operations;

g) an offence committed with terrorist intent, as referred to in chapter 34a, section 1(1)(2–7) or 1(2) of the Finnish Criminal Code;

h) preparation of an offence to be committed with terrorist intent;

i) directing of a terrorist group;

j) promotion of the activity of a terrorist group;

k) provision of training for the commission of a terrorist offence;

l) education of oneself in order to commit a terrorist offence, if the enormity of the offence calls for imprisonment;

m) recruitment for the commission of a terrorist offence;

n) financing of terrorism

o) financing of a terrorist group, if the enormity of the offence calls for imprisonment;

p) travelling in order to commit a terrorist offence, if the enormity of the offence calls for imprisonment.

(chapter 5, section 3 of the Finnish Police Act).

Further, intelligence services by the Finnish Defence Forces are authorised to conduct surveillance solely for the purposes of securing the national territorial integrity (the Finnish Act on the Defence Forces).

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

Exception: If the matter does not brook delay, an official with the power of arrest may decide on traffic data monitoring and on the

obtaining of location data and base station data until such time as the court has decided on the request for the issuing of the warrant (chapter 10 of the Finnish Coercive Measures Act (806/2011 as amended)).

Notwithstanding the above, the police have the right to undertake traffic data monitoring if it is essential that it be conducted straight away to avert an immediate danger to life or health. Further, the police have the right to prevent the use of network addresses or terminal end devices in a certain area for a short period. The use of this action must be essential for the purpose of averting a serious danger to life or health and must not cause more harm or inconvenience than is necessary to carry out the duty (chapter 5, section 8 of the Finnish Police Act).

The police also have the right to obtain base station data if this is necessary for the purpose of averting an imminent danger to life or health (chapter 5, section 11 of the Finnish Police Act).

4. How can intelligence services compel companies to provide access to data?

Under chapter 4, section 3 of the Finnish Police Act and section 44 of the Finnish Act on Military Discipline and Crime Prevention in Defence Forces: “At the request of a commanding police officer, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy.”

In individual cases, the police and the General Staff of the Armed Forces have the right to obtain from a telecommunications operator and a corporate or association subscriber, on request, the contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties.

Under chapter 10, section 63 of the Finnish Coercive Measures Act: "A telecommunications operator shall, without undue delay, make the connections in the telecommunications network necessary for the telecommunications interception and the traffic data monitoring and provide for the use of the criminal investigation authority the information, equipment and personnel necessary for the use of the telecommunications interception. The same applies to situations in which the telecommunications interception or traffic data monitoring is performed by the criminal investigation authority with a technical device. In addition a telecommunications operator shall provide the head investigator with the information in his or her possession that is necessary for the performance of the technical monitoring."

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, to a certain extent. Finland cooperates with Europol, Interpol, and Eurojust. Information on cooperation with other foreign services is classified.

6. Are data subjects notified of surveillance by intelligence services?

Yes, ex post. Under chapter 10, section 60 of the Finnish Coercive Measures Act: "Written notice shall be given without delay to the suspect concerning telecommunications interception, the obtaining of data other than through telecommunications interception, traffic data monitoring, extended surveillance, covert collection of intelligence, technical surveillance and controlled delivery directed at him or her, after the matter has been submitted to the consideration of the prosecutor or the criminal investigation has otherwise been terminated or interrupted. However, the suspect shall be informed at the latest within one year of the termination of the use of a coercive measure."

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes. Data subjects have the right to file an appeal on the grounds of an illegal procedure performed by the authority.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

There is no specific legislation on the subject matter concerning individual surveillance measures.

Pursuant to section 4(a) of the Finnish Act on Police Administration, the Supo shall inform the Finnish Ministry of the Interior and the Chief Director of the Police Force of any material issues belonging to its competence. In accordance with the preparatory works of the Act, the Supo shall also inform the President, the Prime Minister and the Foreign Minister of such issues.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No, we are not aware of any such cases.

11. Do law enforcement authorities need court orders to intercept communications?

Please see answer to question 3 above.

12. How can law enforcement authorities compel companies to provide access to data?

Under chapter 4, section 3 of the Finnish Police Act: "*At the request of a commanding police officer, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy. In individual cases, the police have the right to obtain from a telecommunications operator and a corporate or association subscriber on request contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties.*"

Under chapter 10, section 63 of the Finnish Coercive Measures Act: "*A telecommunications operator shall, without undue delay, make the connections in the telecommunications network necessary for the telecommunications interception and the traffic data monitoring and provide for the use of the criminal investigation authority the information, equipment and personnel necessary for the use of the telecommunications interception. The same applies to situations in which the telecommunications interception or traffic data monitoring is performed by the criminal investigation authority with a technical device. In addition a telecommunications operator shall provide the head investigator with the information in his or her possession that is necessary for the performance of the technical monitoring.*"

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Companies shall not refuse from providing the information if the order is in accordance with the applicable law. Companies have, however,

the right to file an appeal on the grounds of an illegal procedure performed by the authority.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Under chapter 10, section 2 of the Constitution of Finland: “The secrecy of correspondence, telephony and other confidential communications is inviolable.”

Under chapter 1, section 2 of the Constitution of Finland: “The exercise of public powers shall be based on an Act. In all public activity, the law shall be strictly observed.”

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Yes, under the U.S. - EU Privacy Shield.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Generally, yes. All limitations of the secrecy of communications shall be laid down by law. Data subjects have the right to file a claim, on the grounds of applicable law, if their rights have been violated.

17. Are data subjects notified if law enforcement accesses their data?

Yes, ex post. Under chapter 10, section 60 of the Finnish Coercive Measures Act: “Written notice shall be given without delay to the suspect concerning telecommunications interception, the obtaining of data other than through telecommunications interception, traffic data monitoring, extended surveillance, covert collection of intelligence, technical surveillance and controlled delivery directed at him or her,

after the matter has been submitted to the consideration of the prosecutor or the criminal investigation has otherwise been terminated or interrupted. However, the suspect shall be informed at the latest within one year of the termination of the use of a coercive measure."

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Under current legislation, authorities' competence within data acquisition is based solely on crime prevention instead of surveillance. The Supo acts as part of the Police of Finland.

The legislation is currently under reform by the Finnish Ministry of the Interior and the Ministry of Defence. The term of the preparation working groups terminated on 28 February 2017, however, no documentation regarding the results of the preparation has been published yet. We expect that the government bill for new legislation will be introduced this year and that the reform will be partially enacted in late 2017-2018 and enacted in full by 2020 if changes to the Finnish Constitution are required.

According to the Finnish government, the current electronic surveillance legislation does not provide the local law enforcement and defence authorities with adequate powers to combat threats such as terrorism, cybercrime and cyber-attacks and other activities by foreign intelligence services. The government wishes to make it possible to investigate and prevent terrorism and other national security related risks in early stages.

No specific details of the reform have been published but the reform would likely grant the Finnish Defence Forces and the Supo authority to access internet network traffic and conduct electronic mass surveillance for military and civilian intelligence purposes. In addition, the reform is likely to allow new and expanded mobile device location surveillance. The overall purpose of the proposal is to provide Finnish

law enforcement authorities with similar tools that are available in other EU member states.

In addition, new rules on interception may also be introduced in connection with the reform. The Ministry of Justice is preparing a proposal to amend the Finnish Constitution in order to allow legislation which would provide legal framework for intercepting messages, that would otherwise be protected by secrecy of correspondence, if the interception is necessary because of crucial national security reasons.

We also note that section 272 of the Finnish Information Society Code allows surveillance measures taken to implement information security for the purposes of the private sector. Pursuant to the Code, a telecommunications operator, an added value service provider or corporate or association subscriber, or any party acting on their behalf has the right to undertake necessary measures for ensuring information security:

a) in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services;

b) in order to safeguard the possibilities of the sender or recipient of the message for communications; or

c) in order to prevent preparations of means of payment fraud referred to in chapter 37(11) of the Finnish Criminal Code planned to be implemented on a wide scale via communications services.

France

Denise Lebeau-Marianna
Paris
Tel: +33 1 44 17 53 33
denise.lebeau-marianna@bakermckenzie.com

Magalie Dansac Le Clerc
Paris
Tel: +33 1 44 17 59 82
magalie.dansacleclerc@bakermckenzie.com

Hugo Roy
Paris
Tel: +33144176560
hugo.roy@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

France operates both domestic and international surveillance programs.

The legal framework for domestic surveillance is provided for in Title 8 *Du renseignement* ("About Surveillance") of the Code *de la sécurité interne* (Domestic Security Code) (hereafter "CSI").

The French agencies authorized to conduct domestic and international surveillance activities are (L.811-2, L.854-2-III and R. 811-1 CSI):

- the General Foreign Security Office, which is the French foreign intelligence agency (in French Direction *générale de la sécurité extérieure*) (**DGSE**);
- the Defense Intelligence and Security Office (in French the *Direction du renseignement et de la sécurité de la défense*) (**DRSD**) which is an intelligence agency responsible for counter-intelligence and counter-terrorism action. It is part of the Ministry of Defense;
- the Military Intelligence Office which is an intelligence agency responsible of collecting information for the Ministry of Defense (in French the Direction *du renseignement militaire*) (**DRM**);
- the General Domestic Security Office which is the French Domestic Intelligence Agency (in French the Direction *générale de la sécurité intérieure*) (**DGSI**);
- the National Intelligence and Customs Investigation Office which is responsible for intelligence related to customs (in French *Direction nationale du renseignement et des enquêtes douanières*) (**DNRED**); and

- the National service named “intelligence processing and action against clandestine financial circuits” (in French *the Service à compétence nationale dénommé “traitement du renseignement et action contre les circuits financiers clandestins*”) (**TRACFIN**).

In addition, “non-specialized” intelligence services are listed in R. 811-2 CIS and include more than 20 services within the Ministry of Interior and the Ministry of Defence. Other non-specialized intelligence service agencies may be included by Decree within the Ministry of Justice and the Ministry of Economy. Contrary to specialized services, non-specialized intelligence services may only use a limited pre-defined set of intelligence techniques for a limited pre-defined set of purposes (as set forth by Decree).

Implementation of surveillance programs is subject to the authorisation of the Prime Minister following a non-binding recommendation from the National Intelligence Control Commission (in French the *Commission nationale de contrôles des techniques de renseignement* (**CNCTR**) (L 821-1 CSI), except for exceptional emergency situations.

The CNCTR is a newly created body composed of two members of parliament, two senators, two members of the Administrative Supreme Court, two judges and one electronic communications specialist. Its role is to supervise surveillance operations conducted by the French Intelligence Agencies and to issue non-binding recommendations to the Prime Minister.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

Yes.

France’s intelligence services are authorized to conduct both domestic and international surveillance programs justified by threats, risks and stakes linked to the fundamental interests of the nation which include

notably the major economic, industrial and scientific interests of France (L. 801-1 and L. 811-3 CSI).

As surveillance measures are secret, we cannot evaluate the extent to which it has been used to conduct industrial espionage. However, commentators agree that the law gives wide powers to intelligence services.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

No.

Under the new French law on surveillance interception of communications likely to reveal relevant information (L. 852-1 CSI) are subject to an authorization process.

Surveillance measures' authorizations, including communications interception authorization, generally have to follow the following process:

a) The Minister of Defense, the Minister of the Interior, the Minister of Justice, or the Ministers in charge of the Economy, of the Budget or of the Customs (or the persons having delegation of authority) submit a written request of the surveillance measures to the CNCTR (L. 821-2 CSI);

b) The CNCTR issues a non-binding recommendation to the Prime Minister within 24 hours of the receipt of the written request (L. 821 3 CSI);

c) The Prime Minister will then issue an authorization to the minister which requested the implementation of the surveillance measures. This authorization can generally not exceed 4 months in duration (L. 821-1 CSI).

In cases of absolute emergency and only for some explicitly designated purposes, the Prime Minister can issue an authorization

without a prior recommendation from the CNCTR. However, the Prime Minister must inform the CNCTR of the measures taken as soon as possible (L. 821-5 CSI).

The surveillance measures taken may be challenged by the CNCTR or a person affected by such measures or by any jurisdiction before the Administrative Supreme Court (Conseil d'Etat).

The process applicable to international electronic communications surveillance measures does not require a prior recommendation from the CNCTR and may not be challenged by a person before the Administrative Supreme Court.

4. How can intelligence services compel companies to provide access to data?

Intelligence services may compel electronic communications providers and internet hosting providers to provide access to data as defined in Article R. 851-5, subject to the Prime Minister's authorization.

Intelligence services (or law enforcement) may also compel providers of cryptographic services to provide access to data required to decrypt content, in connection with a content interception order (L. 871-1).

Failure for an electronic communications provider or operator (including ISPs, web site editors, hosting providers and telecom operators) to provide intelligence services access to data is a criminal offense.

It is punished by two years of imprisonment for physical persons and by a 150 000-euro fine (multiplied by 5 for companies) (L. 871-2 et L. 881-2 CSI).

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, in particular to fight terrorism, anti-money laundering, drug traffic and more recently cybercriminality

6. Are data subjects notified of surveillance by intelligence services?

No.

It is a criminal offense in France for someone involved in a surveillance program to reveal the existence of this surveillance program (L. 881-1 CSI). It can be punished by a 15 000-Euro fine (multiplied by 5 for companies), a limitation of civil rights, a prohibition from exercising the professional activity within which the surveillance program was conducted, a prohibition to carry a prohibited weapon for 5 years and a publication of the court decision.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes (in general) and No (for international electronic communications surveillance measures).

Any data subject who suspects he/she is kept under surveillance can request the CNCTR to verify the regularity of such measure. The CNCRT will make the appropriate verifications and will give confirmation to the data subject that it has conducted those verifications without revealing to the data subject whether he/she is kept under surveillance (L. 833-4 CSI).

Once the data subject has received an answer from the CNCTR, he/she can request the Administrative Supreme Court of France (in French the *Conseil d'État*) to review the legality of the surveillance operation (L. 841-1 CSI). Should the court decide the surveillance operation has been conducted illegally, it can revoke the authorization to conduct the operation and can order destruction of the data collected (L. 773-7 Code of Administrative Justice, in French *Code de la justice administrative*, hereafter CAJ).

If the Administrative Supreme Court considers the illegality of the surveillance measure could constitute a criminal offense, it can notify

the Republic's prosecutor and provide the CNCTR with the elements of the case in order for the CNCTR to deliver its recommendation to the Prime Minister on the possibility of declassifying these elements in order for them to be transferred to the Republic's prosecutor (L. 773-7 CAJ).

The data subject can also exercise his/her rights related to private data protection by reaching out the French DPA (art. 40 *Loi informatique et libertés*, hereafter **LIL**). In such a case, the Supreme Administrative Court must, if the data is inaccurate, incomplete, ambiguous, out of date or when the collection or processing of this data is prohibited, inform the data subject. The Court can order that this data be rectified updated or erased. The court can decide that the data subject must be indemnified (L. 773-8 CAJ).

However, data subjects do not have a right to court review of international electronic communications surveillance measures (see Constitutional Council, 2015-722 DC of Nov. 26, 2015 and Council of State, no. 397623 of Oct. 19, 2016).

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Not generally.

The only governmental bodies to be notified of the surveillance measures are the Prime Minister, the CNCTR and the Minister who requested the surveillance measure.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Ex-ante: the CNCTR must issue a non-binding recommendation before the Prime Minister who issues an authorization to implement a

surveillance program (except for international electronic communications surveillance programs).

Ex-post: The CNCTR can ask the Administrative Supreme Court for the judicial review of the surveillance measures authorized by the Prime Minister in the case were the Prime Minister has not followed the recommendation issued by the CNCTR or has not given sufficient attention to it (L.833-8 et L.841-1 CSI).

The Administrative Supreme Court of France (in French the *Conseil d'État*) will review the legality of the surveillance operation (L.841-1 CSI). Should the court decide the surveillance operation has been conducted illegally, it can revoke the authorization to conduct the operation and can order destruction of the data collected (L.773-7 CAJ).

If the Administrative Supreme Court considers the illegality of the surveillance measure could constitute a criminal offense, it can notify the Republic's prosecutor and provide the CNCTR with the elements of the case in order for the CNCTR to deliver its recommendation to the Prime Minister on the possibility of declassifying these elements in order for them to be transferred to the Republic's prosecutor (L. 773-7 CAJ)

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes, historically, there have been publicized cases, such as:

- The former director of the DCRI (domestic intelligence service) has been sentenced to a 8,000 EUR fine for unlawful collection of personal data in April 2014 in a case regarding access to communications data (including phone billing data known as "fadettes") of two Le Monde journalists.

- The Elysée Wiretapping Scandal. In the mid 1980s, a series of wiretapping of political enemies, alleging a fight against terrorism was conducted, with the approval of former French President, François Mitterand. Such irregularity was discovered and brought to trial only 20 years later. At that time, no law was regulating the use of wiretapping in France. After the discovery of the scandal, the French legislator adopted a law in 1991, which is now partly codified in the French code of criminal procedure.

- Another famous wiretapping case is called the "Plumbers' case". In the late 1970s, the government put under surveillance the offices of the Canard Enchaîné, a satirical French newspaper. Agents of DGSI dressed as plumbers were discovered by a journalist in the office while installing wiretapping. The different legal actions that the newspaper took were unsuccessful, and the government was never sanctioned.

11. Do law enforcement authorities need court orders to intercept communications?

Yes, the cases where such wiretapping may be authorized by a judge are notably:

- Article 100 of the Code Criminal Procedure (*in French code de procedure pénale*, hereafter **CCP**) provides that if the applicable penalty for a crime is more than two years of imprisonment, the investigating judge can authorize communication interception.

- Article 205 and 283 CCP allow, respectively, the chamber of investigation and the president of the Court of Appeal to authorize interceptions for further investigations.

- Article 706-95 CCP give the ability to the freedom and detention judge (in French "*juge des libertés et de la detention*") to authorize interception during an initial inquiry.

- Article 74-2 CCP also gives the freedom and detention judge the ability to authorize the interception of the communications in order to track a fugitive.\

12. How can law enforcement authorities compel companies to provide access to data?

Article 100-3 CCP states that the investigating judge or officer can request from any telecommunication operator the interception of communications. A decree issued on March 21, 2012 gives a list of all categories of data that can be requested.

Article L. 871-2 CSI states that judicial authorities can order the telecommunication operators to provide any information or documents necessary to conduct lawful interception.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes, though It is not recommended to challenge orders to provide personal data unless if the order is unclear and may be challenged.

Indeed, Article L. 881-1 CSI states that communications operators that refuse to communicate the requested information can be subject to a 150 000-Euro fine (multiplied by five for companies) and a two-year incarceration sentence.

Moreover, the chances of such a challenge to be successful would be limited, notably because of the fact that most information justifying the order will most likely be classified and therefore not available to the companies challenging the order.

However, judicial “warrant” for interception (see Q11 above) may not be challenged (Article 100 CCP).

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Individuals have a general right to privacy and secrecy of correspondences:

- The right to secrecy of correspondences is protected by articles 226-15 and 432-9 of the French Criminal Code.
- The right to privacy is laid down by article 9 of the French Civil Code (applicable to both private parties and governmental bodies) and article 8 of the European Convention on Human Rights (ECHR) (only applicable to governmental bodies).

The French Data Protection act (hereafter **LIL**) ensures protection of individuals when their data is processed by private as well as governmental bodies :

- According to article 38 LIL, any individual can object to the processing or the commercial use of its personal data, except when an explicit provision excludes the application of these provisions;
- Article 39 LIL provides that any individual can request the data controller to obtain information on what data is collected and processed and for what purpose;
- Article 40 LIL states that any individual can ask the data controller to rectify, complete, update, block or erase its personal data, when its inaccurate, incomplete, out of date or when the collection or processing of this data is not relevant or prohibited;
- Article 41 LIL provides that, in derogation to article 39 and 40, when the data is processed for States security, defense or public safety, the individual must request the national commission for information and liberties (CNIL) to verify and, if need be, modify its

personal data. The data is disclosed to the applicant only with the agreement of the data controller;

- Article 42 LIL states that the right to indirect access (article 41 LIL) also applies to the processing carried out by public authorities for the prevention and investigation measures.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

At the moment, the privacy rights are applicable on a territorial basis, not on a citizenship basis. Therefore, French and US citizens have the same protection on French territory. French citizens do not have a global protection.

The LIL is applicable to all entities processing data in France, or to those located outside of the EU and using means of processing in France.

The new EU Privacy Shield should facilitate the EU data subjects to assert their privacy rights against US companies and US government.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Generally Yes, companies can be liable since such disclosure is allowed only on the basis of a justified legal ground.

17. Are data subjects notified if law enforcement accesses their data?

No.

The law provide no obligation, neither ex-ante or ex-post for the judge to notify the data subjects that their communications are or were intercepted.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Yes.

France surveillance laws have undergone several changes since March 2016.

- **Law of June 3rd, 2016 strengthening the fight against organized crime, terrorism and their financing, and improving the efficiency and guarantees of the criminal procedure** (Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale)

Article L. 811-4 CSI now allows services of the Minister of Justice, upon a Decree of the Administrative Supreme Court and after consultation of the CNCTR, to use intelligence techniques provided by the CSI. The list of duly authorized services is specified by a Decree of January 16th, 2017 which modifies accordingly Articles R. 811-2, R. 851-1 to R. 851-4, R. 852-1, R. 8522, R. 853-1, R. 853-2 and R. 853-3 CSI (Décret n° 2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la justice, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure).

Article L. 821-2 CSI now allows the Minister of Justice to submit a written request to the CNCTR with a view that an authorization of the surveillance measure be issued.

- **Law of July 21st, 2016 related to the state of emergency and strengthening counter-terrorism measures** (Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste)

This law significantly amended the following articles:

Article L. 851-2 CSI relates to the collection of real-time information on the networks of operators and electronic communication service providers for the purpose of the prevention of terrorism. It now applies to a wider scope of persons. The requirement that the individual be identified as "posing a threat" is replaced by the condition that it is "likely to be related to a threat". A lower level of dangerousness is thus required. In addition, the collection of real-time information is no longer limited to the person concerned but is extended to persons closely related to him or her where such persons are likely to provide information for the purpose for which the real-time collection authorization was obtained. Also, the authorization for the implementation of this technique is extended from two to four months, thus aligning it with the common duration for intelligence techniques (Article 821-2 CSI).

Article L.852-1 CSI concerning interception of communication content now allows the collection of information "associated" with the interception and not only of the information "necessary" to it. The new wording is thus broader and does no longer require a sorting out of the information.

Article L.863-2 CSI is amended to allow for the sharing of information collected between the various intelligence agencies. To allow a global sharing rather than bilateral exchanges of information, the verb "exchange" is replaced by the verb "to share".

- **Ruling of the Constitutional Council of October 21st, 2016** (Décision n° 2016-590 QPC du 21 octobre 2016)

The legal regime applicable to microwaves interceptions (radio, wireless networks, satellite communications, radar, etc.) applicable since 1991 was declared unconstitutional by the Constitutional Council, which found that such monitoring was not subject to any substantive or procedural requirements and that its implementation

did not provide any guarantee. A new law should be enacted before December 31, 2017.

- **Law of February 28th, 2017 on public safety** (Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique)

This Law creates a new Title within Book VIII of the CSI related to the security intelligence of the penitentiary administration.

The new **Article L.855-1 CSI** extends powers of the penitentiary administration in relation to security intelligence. Penitentiary administration services designated by a Decree of the Administrative Supreme Court after consultation of the National Intelligence Control Commission (CNCTR) may be authorized to use intelligence techniques related to the collection of connection data including electronic communication data (in accordance with articles L. 851-1, L. 851-4, L. 851-5, L. 851-6 and L. 852-1.I) against detained persons, for the purpose of preventing escape, ensuring security and maintain order within prisons and health institutions intended to receive detained persons.

Germany

Joachim Scherer
Frankfurt
Tel: +49 69 2 99 08 189
joachim.scherer@bakermckenzie.com

Caroline Heinickel
Frankfurt
Tel: +49 69 2 99 08 416
caroline.heinickel@bakermckenzie.com

Andreas Neumann
Frankfurt
Tel: +49 69 2 99 08 310
caroline.heinickel@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes. On the federal level there are three intelligence services that operate surveillance programs to protect German national security interests:

- The Federal Intelligence Service (in German: Bundesnachrichtendienst, “BND”) is the German foreign intelligence service. Its legal basis is the Federal Intelligence Service Act (in German: Gesetz über den Bundesnachrichtendienst, “BNDG”).

- The Federal Office for the Protection of the Constitution (in German: Bundesamt für Verfassungsschutz, “BVerfSch”) is the domestic intelligence service of the Federal Republic. Its legal basis is the Federal Constitutional Protection Act (in German: Bundesverfassungsschutzgesetz, “BVerfSchG”).

- The Military Counterintelligence Service (in German: Militärischer Abschirmdienst, “MAD”) is a domestic agency tasked with military counterintelligence. Its legal basis is the Act on the Military Counterintelligence Service (in German: Gesetz über den militärischen Abschirmdienst, “MADG”).

In addition, all sixteen federal states of Germany operate their own domestic intelligence services for the protection of their democratic basic order and their state constitutions.

Apart from the laws cited above, the Law on the Restriction of Privacy of Correspondence, Posts and Telecommunications (in German: Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, “G-10”) is fundamental for the admissibility of telecommunications surveillance in Germany. The G-10 governs all restrictions of the basic right of privacy of correspondence, posts and telecommunications as laid down in Art. 10 of the German Basic Law [Constitution] (e.g. secret recording and interception of

telecommunications). In general, all German intelligence services and law enforcement agencies are bound by the G-10.

Examples for surveillance programs undertaken by the services named above include, inter alia,

- the “Operation Eikonal” (i.e., mirroring of data at the DE-CIX internet exchange point situated in Frankfurt),
- real-time-monitoring of the internet via “in-memory-database”;
- real-time-monitoring of social networks.

2. Are intelligence services authorized to conduct surveillance for an economic purpose

Yes, but the authorization is limited to such economic-related surveillance measures that have a close link to security interests of the Federal Republic. This authorization does not cover activities aimed at protecting undertakings in trade.

In addition, while the BND is empowered to collect and process data regarding telecommunications between foreigners located outside Germany from telecommunications networks located within Germany (so-called “Foreign-Foreign-Surveillance”), industrial espionage is expressly prohibited (Sec. 6 para. 5 BNDG).

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Generally no.

Surveillance measures that limit the constitutional right of privacy of correspondence, posts and telecommunications as laid down in Art. 10 of the German Basic Law (e.g. secret recording and interception of telecommunications) are governed by the G-10 (see question no. 1 above). Such measures must be ordered by the Federal Ministry of the Interior (Sec. 10 G-10) and approved in advance by the G-10-Commission (Sec. 15 G-10). In cases of imminent danger subsequent

approval is sufficient. The G-10-Commission consists of four members, appointed by the German Federal Parliament, who decide independently and are not bound by any instructions whether surveillance measures are necessary and permitted.

Foreign-Foreign-Surveillance measures by the BND (see question no. 2 above) need to be ordered by the Federal Chancellery and approved in advance by the so-called "Independent Body" (see question no. 8 below for details on this body). In cases of imminent danger, subsequent approval is sufficient. The Independent Body's members decide independently and are not bound by any instructions whether surveillance measures are necessary and permitted. Surveillance measures deemed to be inadmissible must be stopped immediately. Similar oversight rules apply to surveillance measures targeted at institutions of the European Union and public institutions of its member states (Sec. 9 BNDG).

The BND is also entitled to conduct "untargeted interception", i.e. mass interception which is not based on the prior suspicion of a specific individual or organization (Sec. 5 to 8 G-10). In such cases, the Federal Ministry of the Interior decides which countries or geographical areas are to be included in a specific untargeted interception measure. This decision must be approved by the PKGr (Sec. 5 para. 1 G-10). In cases of imminent danger subsequent approval is sufficient (Sec. 14 para. 2 G-10).

The German intelligence services are also authorized to request, from companies or private persons, information on certain subjects. Such requests must be ordered

- for the BVerfSch: by the Federal Ministry of the Interior (Sec. 8b para. 1 sen. 2 BVerfSchG);
- for the BND: by the Federal Chancellery (Sec. 3 BNDG);
- for the MAD: by the Federal Ministry of Defense (Sec. 4a MADG).

Finally, if the BVerfSch intends to secretly record a person's private conversation not intended for the public within a dwelling, an approval by the District Court (in German: Amtsgericht) is required unless this would cause undue delay (Sec. 9 para. 2 BVerfSchG).

4. How can intelligence services compel companies to provide access to data?

According to Sec. 2 para. 1 G-10, if so ordered by the intelligence services,

- postal services have to provide information about the circumstances of the postal traffic and to hand out postal items entrusted to them;
- anyone who commercially provides telecommunications services or supports such services is required to disclose information about the circumstances of the communication process and has to enable monitoring and recording of telecommunications.

Non-compliance with such surveillance measures duly ordered by intelligence services triggers administrative fines of up to EUR 15,000 (Sec. 19 para. 1 sent. 1 G-10).

Similar obligations of providers of telecommunications services apply with respect to Foreign-Foreign-Surveillance measures by the BND (Sec. 8 BNDG). Non-compliance in this regard triggers administrative fines of up to EUR 20,000 (Sec. 35 BNDG).

In addition, the BVerfSch may require companies (e.g. air carriers, banks, etc.) or certain private persons to provide information about traffic data and inventory data (Sec. 8a, 8d BVerfSchG).

The same competences have been granted to the BND (Sec. 3, 4 BNDG in connection with Sec. 8a, 8d BVerfSchG) and to the MAD (Sec. 4a, 4b MADG in connection with Sec. 8a, 8d BVerfSchG).

Providers of telecommunications services are required to technically implement surveillance measures and to allow surveillance services to set up respective devices at their premises pursuant to Sec. 110 of the Telecommunications Act (in German: Telekommunikationsgesetz, "TKG"). Operators of telecommunications systems used for the provision of public electronic communications systems have to install intercept capabilities (Sec. 110 para. 1 sent. 1 TKG).

Specified telecommunications providers are required to store certain data related to such allocated numbers/connections (Sec. 111 para. 1 TKG). Furthermore, Sec. 112 and 113 TKG contain rules on an automatic as well as manual procedure for reporting stored data to authorized agencies (e.g. surveillance services and law enforcement authorities).

In the event of non-compliance with these obligations set out in the TKG as cited above, the Federal Network Agency (Bundesnetzagentur, "BNetzA") can impose administrative fines of up to EUR 500,000 on the addressee of the obligation. If the financial benefit derived from the breach exceeds the aforementioned amount, the fine may be even higher (skimming of profits). Furthermore, the BNetzA can enforce compliance through "appropriate" regulatory measures including – as last resort measure and subject to the principle of proportionality – prohibiting the provision of the public telecommunications service in question. The BNetzA may impose enforcement payments of up to EUR 500,000 to enforce fulfilment of these measures.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Under certain circumstances yes, including:

Disclosure of data collected through surveillance measures based on Sec. 5 para. 1 sent. 3 G-10 to foreign services is allowed if

- this is necessary to protect foreign policy or security policy relevant concerns of Germany or significant security interests of another country, and
- there is reciprocity,
- unless legitimate interests of the subject prevent transmission (Sec. 5, 7a, 8 G-10).

Note that such disclosure must be approved by the Federal Chancellery (Sec. 7a para. 1 last sentence G-10).

The BVerfSch may disclose data to foreign services if this is necessary for the fulfillment of its tasks or if there are significant security interests of another country (Sec. 19 para. 3 BVerfSchG).

The BND and the MAD may disclose data to foreign services under the same circumstances as outlined above for the BVerfSch (Sec. 24 para. 2 BNDG and Sec. 11 para. 1 MADG in connection with Sec. 19 para 3. BVerfSchG).

The BND is also entitled to cooperate with foreign intelligence services with regard to Foreign-Foreign-Surveillance measures (Sec. 13 BNDG). Furthermore, the BND may set up joint information files with foreign intelligence services. Collaboration with intelligence services of member states of the EU, the European Economic Area or NATO requires approval by the Federal Chancellery. Collaboration with intelligence services from other countries requires approval by the Chief of the Office of the Federal Chancellery. In addition, the BND may use joint information files provided by foreign intelligence services. This measure requires approval by the Federal Chancellery (Sec. 26 to 30 BNDG).

Finally, the BVerfSch may set up joint information files with foreign intelligence services or use such files provided by foreign intelligence services (Sec. 22b and 22c BVerfSchG). Such collaboration is generally restricted to foreign intelligence services of countries bordering Germany as well as EU and NATO member states. But in

specific cases involving serious criminal offences, the law also allows collaboration with intelligence services of other countries. In any case, the Federal Interior Minister has to approve such collaboration.

6. Are data subjects notified of surveillance by intelligence services?

Generally, yes.

After the completion of surveillance measures based on the G-10 (see question no. 3 above), the affected data subjects should be notified. However, no such notification is required if this would endanger the purpose of these measures or create a disadvantage for Germany or one of its federal states. Also the G-10-Commission can decide to refrain from a notification (Sec. 12 G-10).

Surveillance measures by the BVerfSch are to be notified to the affected data subject unless this would endanger the purpose of these measures or create a disadvantage for Germany or one of its federal states (Sec. 8d para. 3 BVerfSchG). If the BVerfSch secretly records a person's private conversation not intended for the public within a dwelling, the affected data subject must be notified once the measure is completed unless this would endanger its purpose (Sec. 9 para. 3 BVerfSchG).

In addition, the German intelligence services are required to answer information requests by data subjects regarding stored personal data relating to them. Such information requests can be denied without reason if disclosure would create a disadvantage for Germany or one of its federal states or if disclosure would endanger the intelligence services' tasks, public security or the legitimate interests of third parties (Sec. 15 BVerfSchG; Sec. 7 BNDG; Sec. 9 MADG).

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Generally, yes. There are, however, certain restrictions.

Art. 10 para. 2 of the German Basic Law provides that in the case of restrictions of the constitutional right of privacy of correspondence, posts and telecommunications, recourse to the courts may be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature if such restriction serves to protect the free democratic basic order or the existence or security of the German Federation or of one of its States.

In order to challenge surveillance orders issued by the BND, MAD or BVerfSch pursuant to Sec. 2 para. 1 G-10, the data subject may file a complaint with the administrative courts. In cases of surveillance measures based on the G-10 (see question no. 3 above), court review is only possible once the affected data subject has been officially notified of these measures (Sec. 13 G-10).

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes.

The German intelligence services are subject to supervision by the Federal Government. The competent governmental bodies for this supervision are the Federal Ministry of the Interior (for the BVerfSch), the Federal Chancellery (for the BND) and the Federal Ministry of Defense (for the MAD).

In addition, the activities of the BVerfSch, BND and MAD as well their supervision by the Federal Government are controlled by the Parliamentary Control Panel (in German: Parlamentarisches Kontrollgremium, “PKGr”). The PKGr is based on the Control Panel Act (in German: Kontrollgremiumgesetz, “PKGrG”) and currently consists of nine members, elected from among the members of the German Parliament for the duration of its mandate. The Federal Government is required to inform the PKGr about the general activities of the intelligence services and about events of particular

significance. The PKGr also can request the Federal Government to produce special reports (Sec. 4 PKGrG). The reporting requirement is not limited to ex post notification. The Federal Government has to notify the PKGr in advance and/ or during surveillance operations in cases of special political sensitivity and if there is serious interference in a person's basic rights. The PKGr files a report with the German Parliament on its monitoring activity. The PKGr also decides - together with the Federal Ministry of the Interior - about the countries or geographical areas that are to be included in untargeted interception by the BND (see question no. 3 above).

Surveillance measures based on the G-10 (see question no. 3 above) have to be reported to the PKGr at least every six months. The PKGr has to submit an annual report on these measures to the German Bundestag (Sec. 14 G-10).

In addition, surveillance measures based on the G-10 need to be approved in advance by the G-10-Commission (Sec. 15 G-10). Consequently, the G-10-Commission must be notified of any such measures. The G-10-Commission consists of a chairman who must be qualified for judicial office and three other full members as well as four substitute members. The G-10-Commission's members are appointed for the duration of the German Parliament's mandate by the PKGr after consulting the Federal Government.

Note that "Foreign-Foreign-Surveillance" measures by the BND (see question no. 2 above) need not to be approved by the 10-G-Commission. Instead, such surveillance measures are controlled by the so-called "Independent Body" (in German: Unabhängiges Gremium). The Independent Body consists of a chairman, two other full members as well as three substitute members. The members are Supreme Court judges and prosecutors of the Federal Prosecutor's Office who are appointed by the Federal Cabinet for a six year term upon proposals by the president of the Supreme Court and the Federal Prosecutor General, respectively.

If the BVerfSch requires companies (e.g. air carriers, banks, etc.) or certain private persons to provide information about traffic data and inventory data (Sec. 8a BVerfSchG), the Federal Ministry of the Interior has to inform the G-10-Commission on a monthly basis before the execution of such measures (Sec. 8b para. 2 BVerfSchG). The Federal Ministry of the Interior also has to inform the PKGr at least every six months about the execution of such measures (Sec. 8b para. 3 BVerfSchG).

In addition, any secret recording of a person's private conversation not intended for the public within a dwelling by the BVerfSchG has to be reported to the PKGr (Sec. 9 para. 3 no. 2 BVerfSchG).

The MAD may gather information during a foreign assignment of the German military. Such activities are, however, limited to the territory of Germany and to the confines of German military camps abroad. Such activities of the MAD must be notified in advance by the Federal Government to the PKGr (Sec. 14 MADG).

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

This depends on the oversight body in question. For details on ex ante or ex post notification requirements, see question no. 8 above.

Oversight by the PKGr usually occurs after a surveillance measure has been taken. This is also due to the fact that the PKGr usually only meets four times per year. However, the Federal Government has to notify the PKGr in advance and/or during surveillance operations in cases of special political sensitivity and if there is serious interference in a person's basic rights.

The Independent Body was established in the beginning of 2017. It is to be expected that – similar to the PKGr – oversight by the Independent Body will mostly occur after a surveillance measure has been taken since the Independent Body is scheduled to meet only

four times per year. However, the Federal Chancellery has to notify the Independent Body in advance about Foreign-Foreign-Surveillance measures.

The G-10-Commission's oversight powers with regard to surveillance measures covered by the G-10 include the collection, processing and use of personal data obtained under the G-10 as well as the decision whether the data subject should be notified (Sec. 15 para. 5 G-10).

The governmental bodies with legal and professional supervision over the intelligence services – as mentioned in question no. 8 above – have a right to object to (individual) surveillance measures.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes.

A publicized case of violation of the German law on intelligence services includes the "Operation Eikonal". This was a collaboration between the NSA and the BND to mirror all data at the DE-CIX internet exchange point situated in Frankfurt between 2004 and 2008. The clarification of this operation is still in progress.

Another publicized case of violation of the German law on intelligence services is the so-called "spying-on-journalists scandal". In the period from 1993 to 1998, the BND has monitored various German journalists who were known to be critical of the BND. Allegedly, neither the PKGr nor the Federal Chancellery had been informed about these surveillance measures. A parliamentary investigation committee was set up to clarify what happened. As a consequence, the Federal Chancellery instructed the BND to stop these surveillance measures.

11. Do law enforcement authorities need court orders to intercept communications?

Generally, yes.

Law enforcement authorities need court orders to intercept communications as laid down in Sec. 100b para. 1 of the Code of Criminal Procedure (in German: Strafprozessordnung, "StPO"). However, in cases of imminent danger the interception of communications may be also ordered by the public prosecutor's office. Such administrative interception orders expire within three days unless they are confirmed by a court. The results of these surveillance measures are to be reported to the ordering court after their completion (Sec. 100b para. 4 StPO).

Surveillance measures by the German Federal Criminal Police Office (in German: Bundeskriminalamt, "BKA") also require a court order. In cases of imminent danger, the interception of communications may be ordered by the Director of the BKA. Such interception orders expire within three days unless they are confirmed by a court (Sec. 20l of the Law on the Federal Criminal Police Office (in German: Bundeskriminalamtsgesetz, "BKAG").

Regarding violations of the Foreign Trade Act and the War Weapons Control Act, there is a special legal basis for surveillance measures by the Customs Investigation Services (in German: Zollfahndungsämter). According to Sec. 23a of the Law on Customs Investigation Services (in German: Zollfahndungsdienstgesetz, "ZFdG") these authorities may inspect postal items as well as monitor and record telecommunications if there is a court order. However, in cases of imminent danger such surveillance measures may be ordered by the Federal Ministry of Finance. Such administrative surveillance orders expire within three days unless they are confirmed by a court (Sec. 23b ZFdG).

12. How can law enforcement authorities compel companies to provide access to data?

Anyone who provides telecommunications services or supports such services must cooperate with the court, the public prosecutor's office and police officers following an interception order (see question no. 11 above). This means that companies covered by this obligation must enable the implementation of surveillance measures and provide all relevant information (Sec. 100b para. 3 StPO).

If companies do not meet their obligation to support surveillance measures as outlined above, the court may impose coercive measures, e.g. administrative fines or even imprisonment (Sec. 100b para. 3 last sentence in connection with Sec. 95 para. 2 StPO).

Law enforcement authorities are also entitled to seize data storage media of companies (e.g. hard drives or USB flash drives) pursuant to Sec. 94 StPO.

In the case of surveillance measures by the Customs Investigation Services, companies are required to meet the obligations set out in Sec. 2 para. 1 G-10 (see question no. 4 above).

As far as the technical implementation of surveillance measures (e.g. installation of respective software, etc.) as well as obligations for companies under the TKG related thereto are concerned, please see question no. 4 above.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Companies that are ordered to implement surveillance measures pursuant to Sec. 100b StPO have a right to court review. However, review is limited to aspects of the technical implementation of such surveillance measures and the companies' obligations related thereto. This means that companies are not entitled to object to individual surveillance measures in general. Especially, companies cannot

safeguard the interests of the affected data subjects (relevant case law: Regional Court Hildesheim, decision of 21.4.2010, case no. 26 Qs 58/10; Regional Court Bielefeld, decision of 1 December 2003, case no. Qs 495-498/03 IX).

In addition, court orders can be reviewed by the Federal Constitutional Court for violation of constitutional rights.

Examples of challenged orders:

- Appeal by providers of telecommunications services against the obligation to provide information about IP-addresses (Federal Constitutional Court, decision of 13 November 2010, case no. 2 BvR 1124/10).
- Appeal by a provider of telecommunications services against the obligation to intercept certain telephone communications (Higher Regional Court Frankfurt/Main, decision of 30 November 2006, case no. 20 W 128/05).

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Privacy rights of individuals against the government are found, in particular, in the following provisions:

- Constitutional right of privacy of correspondence, posts and telecommunications as laid down in Art. 10 of the German Basic Law;
- Constitutional right of privacy (informational self-determination) under Art. 2 Sec. 1 of the German Basic Law;
- Right to respect for one's private and family life, his home and his correspondence pursuant to Art. 8 of the European Convention on Human Rights ("ECHR");

- Sec. 12 to 26 of the Federal Data Protection Act (in German: Bundesdatenschutzgesetz, “BDSG”).

Privacy rights of individuals against companies that share personal data with the government are found, in particular, in the following provisions:

- Sec. 11 to 15a of the Telemedia Act (in German: Telemediengesetz, “TMG”);
- Sec. 27 to 35 BDSG;
- Sec. 201 to 206 of the Criminal Code (in German: Strafgesetzbuch, “StGB”;
- Sec. 88 et seq. TKG.

Please note that Art. 10 of the German Basic Law as well as Art. 8 ECHR are not applicable to non-governmental actors.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

The BDSG is not only applicable to data processing entities in Germany, but also to those seated outside the European Union (Sec. 1 para. 5 second sentence BDSG). Such foreign entities (e.g. U.S. companies) are subject to all obligations set out by the BDSG provided that they collect, process and use data within Germany. The same applies to data protection obligations set out in the TKG and TMG. Under these circumstances data subjects may assert privacy rights against U.S. companies or the U.S. government.

Conversely, this means that U.S. companies or the U.S. government are not covered by German data protection rules as long as they refrain from collecting, processing and using data within Germany.

Finally, please note that the former U.S.-EU Safe Harbor Program which was declared invalid by the European Court of Justice on 6

October 2015 (case no. C-362/14) has been replaced by the EU-US Privacy Shield since July 2016.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes. If companies disclose data to the government without sufficient legal bases, the affected data subjects may assert, inter alia, the following claims:

- damage claims pursuant to Sec. 7 BDSG due to violations of the obligations set out in the BDSG;
- damage claims pursuant to Sec. 44 TKG due to violations of the obligations set out in the TKG;
- damages claims for the breach of contractual obligations (if applicable) according to the principles of German contracts law;
- damage claims for the violation of general personality rights pursuant to Sec. 823 para 1. of the Civil Code (in German: Bürgerliches Gesetzbuch, "BGB").
- finally, damage claims for the violation of data protection obligations can be generally based on Sec. 823 para. 2 BGB.

17. Are data subjects notified if law enforcement agencies accesses their data?

Generally, yes.

Data subjects affected by surveillance measures undertaken by law enforcement agencies have to be notified (Sec. 101 para. 4 StPO). However, such notification must not be provided if this would endanger (i) the purpose of the surveillance measures, (ii) the life, physical integrity or freedom of persons, or (iii) significant assets (Sec. 101 para. 5 StPO). Authorities may refrain from notification due to the

aforementioned reasons up to one year after completion of the surveillance measures. Any further postponement of the notification needs to be approved by the court. If it is virtually certain that the reasons cited above will persist, the court may even decide to abstain from notification permanently (Sec. 101 para. 6 StPO).

In the case of surveillance measures by the Customs Investigation Services, data subjects also have to be notified unless this would endanger (i) the purpose of the surveillance measures, (ii) the life, physical integrity or freedom of persons, or (iii) significant assets (Sec. 23c para. 4 ZFdG).

Similar notification requirements apply to surveillance measures by the BKA (Sec. 20b para. 6 BKAG, Sec. 20w BKAG).

Hong Kong

Paolo Sbuttoni
Hong Kong
Tel: +852 2846 1521
paolo.sbuttoni@bakermckenzie.com

Gillian Lam
Hong Kong
Tel: +852 2846 1686
gillian.lam@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

No.

We take “intelligence services” to mean “intelligence agencies” such as the CIA or MI5.

Hong Kong, being a special administrative region of China, does not have its own bureau/department that is responsible for national security. In China, the intelligence agency will be the Ministry of State Security.

Based on Article 14 of the Hong Kong Basic Law, the Central People’s Government shall be responsible for the defence of the HKSAR and the Government of the Hong Kong Special Administrative Region shall be responsible for the maintenance of public order in the Region. Military forces stationed by the Central People’s Government in the Hong Kong Special Administrative Region for defence shall not interfere in the local affairs of the Region.

In Hong Kong, there are law enforcement agencies which have intelligence functions dedicated to combatting crimes or terrorism, such as the Criminal Intelligence Bureau (CIB) which is a branch of the Hong Kong Police Force and the Joint Financial Intelligence Unit (JFIU), which is jointly operated by the Hong Kong Police Force and the Customs and Excise Department.

The CIB cultivates information in relation to criminal activities, societies, organized and serious crime. It conducts research on such activities and mounts intelligence-based operations against the syndicates involved, enabling strategic and tactical intelligence to be produced for enforcement action mainly by the OCTB and regional crime formations. The Bureau also has a dedicated role in kidnapping and terrorist incidents. See http://www.police.gov.hk/ppp_en/01_about_us/os_cs.html

The JFIU manages the suspicious transaction reports (STRs) regime for Hong Kong and its role is to receive, analyse and store suspicious transactions reports (STRs) and to disseminate them to the appropriate investigative unit. See http://www.jfiu.gov.hk/en/aboutus.html

2. Are intelligence services authorized to conduct surveillance for an economic purpose

Not applicable. (Please see Section 1)

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Not applicable. (Please see Section 1)

4. How can intelligence services compel companies to provide access to data?

Not applicable. (Please see Section 1)

5. Are national intelligence services cooperating and exchanging information with foreign services?

Not applicable. (Please see Section 1)

6. Are data subjects notified of surveillance by intelligence services?

Not applicable. (Please see Section 1)

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Not applicable. (Please see Section 1)

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of

(individual) surveillance measures taken by intelligence services?

Not applicable. (Please see Section 1)

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable. (Please see Section 1)

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Not applicable. (Please see Section 1)

11. Do law enforcement authorities need court orders to intercept communications?

Yes. The interception by or on behalf of any officer must be authorized by a panel judge who must be a Court of First Instance Judge. The Hong Kong Police, Customs and Excise Department and the Independent Commission Against Corruption (ICAC)[6] may apply to a panel judge for such authorization[7].

However, exceptions apply allowing for executive authorizations in cases of emergency[8].

[6] This is Hong Kong's anti-corruption government unit. It has an investigative function and has powers of search and seizure as well as the powers of arrest and detention. See http://www.icac.org.hk/en/about_icac/le/index.html

[7] Section 8, Interception of Communications And Surveillance Ordinance (ICSO) (Cap 589)

[8] Section 20, ICSO (Cap 589)

12. How can law enforcement authorities compel companies to provide access to data?

Hong Kong Police Force (HKPF): a warrant is needed by a magistrate to enter/break into a premise to search for and take possession of any newspaper, book or other document or any portion or extract, or any other article or chattel[9]. Alternatively, a police officer can search for and take possession of such documents from an apprehended person if he reasonably suspects the document to be of value to the investigation of any offence that the person has committed or is reasonably suspected of having committed[10].

Securities and Futures Commission[11] (SFC) and Hong Kong Monetary Authority (HKMA): Under the Securities and Futures Ordinance (SFO), the SFC or the HKMA can compel persons under investigation to produce any record or document specified by the investigator relevant to the investigation[12]. Further, with magistrate's warrants, SFC or HKMA officers may enter premises and seize records/documents from the premises if there are reasonable grounds to suspect that there is any document or record which may be required to be produced under the SFO[13].

Independent Commission Against Corruption (ICAC). The ICAC officer may search premises and seize anything which he has reason to believe to be or to contain evidence of any offences referred under section 10 of the ICAC Ordinance[14].

[9] Section 50(7)(a), Police Force Ordinance (Cap 232)
[10] Section 50(6), Police Force Ordinance (Cap 232)
[11] The Securities and Futures Commission (SFC) is an independent statutory body set up in 1989 to regulate Hong Kong's securities and futures markets. Its investigative, remedial and disciplinary powers are derived from the Securities and Futures Ordinance (Cap 571) (SFO). See http://www.sfc.hk/web/EN/about-the-sfc/our-role/
[12] Section 183 and 184B, SFO
[13] Section 191, SFO
[14] Section 10B, ICAC Ordinance

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes. The decision to issue a search warrant is susceptible to challenge by judicial review unless the court which issued the warrant was the Court of First Instance.

The basis for judicial review include error as to jurisdiction, improper and irrelevant policy, the application of the threshold criteria was too low or too high, irrational decision, bias and irrelevant considerations taken into account[15].

For SFC and HKMA: It is a crime if a person fails to produce records or documents compelled under the investigation or search warrant directed by the magistrate, unless there is reasonable excuse[16]. However, the reasonable excuse is very narrow and applies only to cases such as physical inability to produce information[17].

The Privacy Commissioner provided guidance on disclosure of customers' personal data to law enforcement agencies[18]. When companies handle requests for disclosure of customer personal data from law enforcement agencies, they should ask the enforcement agencies the purpose of which the data is used, why the data is considered necessary or important for that purpose and, in particular, how the failure to disclose the data would be "likely to prejudice" any such matter[19]. If the disclosure of customers' personal data to a law enforcement agency is not directly related to the original purposes of the collection of the data, the company should not make the disclosure unless prescribed consent has been obtained.

[15] Paragraph 130.606, Halsbury's laws of Hong Kong (2016)
[16] Section 185(1), SFO
[17] Bank of England v Riley [1990]
[18] Paragraph 3.7, Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry (https://www.pcpd.org.hk/english/publications/files/GN_banking_e.pdf)
[19] Section 58(2)(b), PDPO

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against government: Art. 39 of the Basic Law makes clear that the International Covenant on Civil and Political Rights (ICCPR) apply to Hong Kong. Art.17 of the ICCPR protects the right to privacy from governmental interference. On the grounds of illegality due to contravention of the Basic Law, governments can be subject to judicial review by the court. The court reviews the lawfulness of a decision, action or failure in relation to the exercise of a public function[20].

Against companies: Under s. 4 Personal Data (Privacy) Ordinance (PDPO), a data user (i.e. companies) shall not do any acts that contravene a data protection principle (DPP). DPP 3 prevents personal data to be used for a new purpose without the express voluntary consent of the data subjects (the individuals). An individual can lodge complaint to the Privacy Commissioner. (s.37 PDPO) The Commissioner then investigates complaints against data users (i.e. companies) and can serve an enforcement notice directing the data user to carry out remedial action if he believes that the data user has contravened legislative requirements.

However, personal data is exempted from DPP 3 if data is used for the purposes of safeguarding security, defence or international relations (s.57(2) of PDPO); for prevention, assessment and preclusion of crime (s.58(2) PDPO). Further, personal data which is or is contained in an interception product (i.e. any contents of a communication that have been obtained pursuant to a prescribed authorization for interception) or in a surveillance product (i.e. any material obtained pursuant to a prescribed authorization for covert surveillance) is also exempted from the provisions of the PDPO.

[20] Paragraph 90.1098, Halsbury's laws of Hong Kong (2016)

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

In addition to lodging a complaint to the Privacy Commissioner which could issue an enforcement notice[21], the data subjects can institute civil proceedings against companies if they have suffered damages as a result of a contravention of the present ordinance. There is a relevant case in Hong Kong concerning a bank which has disclosed a customer's personal data to a third party (an insurance company) for marketing purpose[22]. The Privacy Commissioner issued an enforcement notice against the bank and the bank appealed. The Court dismissed the appeal and held that disclosing the personal data to the insurance company was not within the original purpose of collecting the personal data from the client.

17. Are data subjects notified if law enforcement accesses their data?

DPP 1 of the PDPO requires the data subject be explicitly or implicitly informed on or before collecting the data. DPP 3 of the PDPO implicitly requires express voluntary consent of the data subject to be sought before it is used for a new purpose.

However, as noted under Q 14, there are exemptions.

[21] Section 37, PDPO
[22] *Wing Lung Bank Ltd V Privacy Commissioner For Personal Data* [2010] 6 HKC 266

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

For law enforcement agencies: The Interception of Communications and Surveillance (Amendment) Ordinance 2016 came into force on 24 June 2016, which empowers the Commissioner on Interception of Communications and Surveillance to examine, inspect and listen to protected products including those which concern cases of non-compliance or irregularity and cases involving information that is subject to legal professional privilege[23].

[23] http://www.legco.gov.hk/yr15-16/english/ord/ord021-2016-e.pdf; http://www.legco.gov.hk/yr14-15/english/hc/papers/hc20150227ls-39-e.pdf; http://www.legco.gov.hk/yr15-16/english/panels/se/papers/se20151201cb2-327-1-e.pdf

Hungary

Ines K. Radmilovic
Budapest
Tel: +36 1 302 3330
ines.radmilovic@bakermckenzie.com

Adam Liber
Budapest
Tel: +36 1 302 3330
adam.liber@bakermckenzie.com

Janos Puskas
Budapest
Tel: +36 1 302 3330
janos.puskas@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

In general, yes. However, the Hungarian Department of Justice may also order such interception and the intelligence services tend to leverage this opportunity. However, an amendment of the relevant Hungarian regulations is expected following the European Court of Human Rights' ruling that the Department of Justice's authorization to issue surveillance orders is unlawful.

4. How can intelligence services compel companies to provide access to data?

Through court orders or orders of the Department of Justice.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes. Hungarian intelligence services cooperate and exchange information with services of other NATO and EU countries.

6. Are data subjects notified of surveillance by intelligence services?

In practice, no.

If a court authorized the surveillance prior to the launch of a formal criminal investigation and no criminal procedure is initiated against the surveilled person, the public prosecutor must notify the data subject

about the occurrence of the surveillance, unless such disclosure could jeopardize the criminal investigation. If a criminal procedure is initiated against the surveilled person, in most cases the public prosecutor must disclose to the accused person the report about the surveillance and the court's decision authorizing the surveillance activity.

Hungary plans to amend the rules governing notifications to surveilled data subjects; consequently, the above rules might be amended in the near future.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

No.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No.

The National Security Committee of the Hungarian Parliament may ask the national intelligence services to provide them with information about certain cases, including the surveillance which applicable law does not require be reported to the data subject, but no automatic notification to the Committee is required.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws

relating to surveillance measures? What were the consequences? Name examples.

Yes. If the national intelligence services violate applicable laws relating to surveillance measures, the illegally or improperly obtained evidence may not be used in the criminal procedure.

11. Do law enforcement authorities need court orders to intercept communications?

In general, yes. However, the Department of Justice may also order such interception and the law enforcement authorities tend to rely on this. The law enforcement authorities may not proceed with the interception themselves; they must request the intelligence services' technical assistance.

However, an amendment of the relevant Hungarian regulations is expected following the European Court of Human Rights' ruling that the Department of Justice's authorization to issue surveillance orders is unlawful.

12. How can law enforcement authorities compel companies to provide access to data?

By law enforcement orders, which may be issued only to companies domiciled in Hungary. Failure to provide the data in response to a law enforcement order may result in a default fine being assessed. Hungarian law enforcement authorities may require access to data hosted by foreign companies only through the applicable international legal assistance procedures.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

A complaint may be filed with the public prosecutor within 8 days. However, this legal remedy has no suspensive effect on the requirement to provide the personal data.

The decision of the public prosecutor requiring the provision of data may not be challenged in court.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

An individual may file a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) or seek a remedy in civil court based on a privacy rights breach. In the court action, the data subject may claim damages. In practice, neither of the above actions is effective in the surveillance context.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

No as to U.S. government, which enjoys immunity before Hungarian courts (unless the U.S. government expressly waives / disclaims its immunity).

Yes as to U. S. companies. U.S. companies are responsible for the processing of European data subjects' personal data. The publicly available court rulings suggest that Hungarian data subjects actually exercise their privacy rights against U.S. companies before Hungarian courts.

U.S. individuals may enforce their privacy rights before Hungarian courts.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes; disclosure in the absence of a sufficient legal basis is a privacy rights breach, which may have both civil and criminal law consequences.

17. Are data subjects notified if law enforcement accesses their data?

In practice, no.

Some regulations provide narrow notification obligations to data subjects concerning law enforcement procedures, but, in practice, data subjects are typically not notified. Amendments to Hungary's regulations concerning notification obligations concerning personal data access are expected.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

In 2016 Hungary implemented intrusive and stringent surveillance and encryption regulations in the context of online communications.

With an unusually broad extraterritorial scope, the new rules apply to companies that make available to Hungarian private and business users any online or other electronic communication channels, regardless of whether such company is domiciled in Hungary. Companies providing web or mobile based audio or video communications, e-mail, instant messaging or social media services are likely affected by the new rules.

Companies subject to the new rules are required to retain certain metadata (such as user IDs, times of registration and access, and IP addresses) for one year and disclose such data in response to targeted data / surveillance requests from Hungarian intelligence

services. Law enforcement authorities may channel their requests for user data only through the intelligence services.

The retention and disclosure obligations apply regardless of product features. Consequently, companies might be required to change product features in order to get access to their users' metadata. These current rules seem to prohibit end-to-end encryption of metadata.

That said, companies may choose whether or not they encrypt end-to-end the actual content of communications and influence their disclosure obligations by doing so. Online communications companies whose service is deemed non end-to-end encrypted for purposes of the current rules can be requested to monitor specific users' full text, audio or video communications content and to disclose it to the authorities. By contrast, companies that encrypt end-to-end the actual content of communications will only be required to disclose the metadata mentioned above.

The government decree issued in connection with the current surveillance regulations imposes restrictions on product feature changes and other changes by online communication providers, if such changes might impede user surveillance.

Online communication providers failing to follow the current rules face a new regulatory enforcement procedure and fines of up to HUF 10 million (approximately US$35,000) per offence.

India

Probir Roy Chowdhury
Bangalore
Tel: +91-80-43503618
probir@jsalaw.com

Sajai Singh
Bangalore
Tel: +91-98450 78666
sajai@jsalaw.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

No, however intelligence agencies would require approval from the Ministry of Home Affairs of the Central Government, or the Secretary to the appropriate State Government in charge of the Home Department.

4. How can intelligence services compel companies to provide access to data?

This may be through several means, including:

Through court orders; and

Through direct orders issued under enabling legislations. For example, under Section 165 of the Code of Criminal Procedure, a police officer conducting an investigation has been conferred the power of search any premises and seize any relevant material or information found. Similarly, under Section 69 of the Information Technology Act, 2000 ("IT Act"), the Central Government or State Government may order the owner of a computer resource (including a computer or electronic database) to provide any information stored on such computer resource.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, for example, the Central Bureau of Investigations (CBI) has been notified as the Interpol for India. Consequently, the CBI acts as an interface between the law enforcement agencies of India and other countries to ensure cooperation and facilitates exchange and sharing of information by these agencies. It also facilitates execution of Letters of Request for Investigation in India and out of India.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

The right to privacy has been recognized as a fundamental right by Indian courts. Therefore, a citizen of India may approach a court, if he/she believes that his/her right to privacy has been infringed upon by any surveillance measures taken by intelligence services.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes, in most cases, surveillance measures (such as phone tapping) require the approval of the Ministry of Home Affairs of the Central Government, or the Secretary to the appropriate State Government in charge of the Home Department.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Since prior approval is required (as discussed above), notification of proposed surveillance measures would have to be made ex ante.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes. For example, in the case of People's Union for Civil Liberties (PUCL) v. Union of India, which pertained to certain unlawful surveillance and phone tapping activities carried on by the CBI, the Supreme Court of India issued guidelines for the prevention of arbitrary surveillance, interception and monitoring activities by Indian intelligence and law enforcement authorities.

These guidelines were later incorporated into the Indian Telegraph Rules, 1951, in Rule 419 A, which prescribes multiple safeguards to prevent unnecessary or arbitrary interception and monitoring of telephone messages.

11. Do law enforcement authorities need court orders to intercept communications?

No. Similar to intelligence agencies, law enforcement authorities require approval from the Ministry of Home Affairs of the Central Government, or the Secretary to the appropriate State Government in charge of the Home Department in order to intercept communications.

12. How can law enforcement authorities compel companies to provide access to data?

Indian law enforcement authorities can compel companies to provide access to data in the same manner as intelligence agencies.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes, a company may challenge orders to provide personal data to law enforcement authorities. Under Section 482 of the Code of Criminal Procedure, 1973 ("CrPC"), the High Court of a State may issue any order as deemed necessary to prevent abuse of the processes of the court or otherwise to secure the ends of justice. Consequently, a company may approach a High Court under Section 482 of the CrPC, to challenge any order issued by law enforcement authorities.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against Government: An individual may file a writ petition for the enforcement of his right to privacy (guaranteed under Article 21 of the Constitution of India).

Against Companies: An individual may proceed against the company under Section 43A of the IT Act, to recover damages for any loss caused or injury suffered.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Yes, a European data subject may assert privacy rights against Indian companies, under Indian laws. However, it is unlikely that such rights may be successfully asserted against the Indian Government.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes, a company would be liable under Section 43A of the IT Act, however, no examples have been reported in this regard.

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

None.

Indonesia

Hendronoto Soesabdo
Jakarta
+62 21 2960 8610
hendronoto.soesabdo@bakernet.com

Reno Hirdarisvita
Jakarta
Tel: +62 21 2960 8571
reno.hirdarisvita@bakernet.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

Note: For the purpose of this questionnaire, state intelligence services in Indonesia is carried out by: (i) the State Intelligence Agency (*Badan Intelijen Negara* - "**BIN**"); (ii) Intelligence at the National Armed Forces (*Tentara Nasional Indonesia*/TNI); (iii) Intelligence at the Police Force of the Republic of Indonesia; (iv) Intelligence at the Prosecutor Offices of the Republic of Indonesia; and (v) Intelligence at the ministries/non-ministerial government agencies. Intelligence services in Indonesia carried out by these bodies are coordinated by BIN.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

Indonesian laws do not specifically regulate the concept of industrial espionage. However, Law No. 17 of 2011 on State Intelligence ("**State Intelligence Law**") provides that BIN has the authority to (i) conduct wiretapping on; (ii) investigate flow of funds of; and (iii) uncovering information from a party involved in activities threatening national economy.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

BIN can intercept calls, emails or other communications by order from the head of BIN. BIN will need to obtain a court order to intercept a target if BIN has obtained sufficient preliminary evidence against the target.

4. How can intelligence services compel companies to provide access to data?

Through an order from the head of BIN

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes. Malaysia, Indonesia and Singapore have an intelligence sharing framework for regional security. Another example is Indonesia's renewal of its intelligence cooperation with Australia on terrorism.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes. Data subjects whose rights are infringed may lodge a request of rehabilitation, compensation and restitution for the damages that have incurred arising from the surveillance measures taken by the intelligence services. However, the State Intelligence Law does not specify whether the request should be made to the court. Furthermore, there is yet a legislation regulating the procedure for this request.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Indonesian prevailing laws and regulations are silent on this. BIN is directly accountable only to the President of Indonesia.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

N/A

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

No, but must be done based on an order from an authority (police, prosecutor and/or other agency with law enforcement authority).

Law No. 36 of 1999 on Telecommunications ("**Telecommunications Law**") provides that for the purposes of criminal proceedings, intercepting of communications can be done (i) with a written order from the Attorney General or the Chief of the Police Force; or (ii) by request of the investigator investigating the case. However, to date there is no legislation specifically regulating the procedure for intercepting communications.

Law No. 11 of 2008 on Electronic Information and Transaction as amended by Law No. 19 of 2016 ("**EIT Law**") further provides that in order for electronic information and/or documents which are obtained through interception or wiretapping, to be deemed as valid evidence, the interception or wiretapping must be done for the purposes of law enforcement through the request of the police, prosecutor and/or other institutions whose authority is determined by the law.

12. How can law enforcement authorities compel companies to provide access to data?

Court orders.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Indonesian prevailing laws and regulations are silent on any avenues for companies to challenge orders to provide personal data to law enforcement authorities.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Indonesia does not have a specific privacy law. However, privacy is regulated under several laws, among others, the EIT Lawand Law No. 39 of 1999 on Human Rights ("**Human Rights Law**").

Privacy rights against government agencies:

The prevailing laws do not provide individuals with privacy rights against government agencies if their personal data is shared with the government.

Having said that, if any personnel of a state intelligence services abuses the authority to intercept communications, such personnel may face criminal sanctions pursuant to Article 47 of the State Intelligence Law

Privacy rights against companies:

Any person whose rights are infringed may lodge a claim for any damages that are incurred arising from the unauthorized use of their private or personal data. Such person can lodge a civil claim against the party who uses their personal data without any consent

The Minister of Communication and Informatics ("**MOCI**") has recently issued Minister of Communication and Information Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System ("**MOCI Regulation 20**").

Article 29 of MOCI Regulation 20 provides that the owner of personal data may submit a complaint to MOCI if a written notice is not sent by an electronic system administrator to the owner of the personal data regarding the failure to protect personal data which may or may not potentially create a loss. Alternatively, a complaint may also be filed if there is a failure to protect personal data but the written notice was not sent in a timely manner.

Additionally, Article 36 of MOCI Regulation 20 provides that administrative sanctions may be imposed to those who obtain, collect, process, analyze, store, announce, send and/or distribute personal data contrary to the prevailing laws and regulations in the form of (i) verbal warning, (ii) written warning, (iii) temporary suspension of activities and/or, (iv) announcement in an online website.

Following the issuance of MOCI Regulation 20, a draft bill is currently being drafted on the protection of personal data.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

N/A

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes, companies are generally liable for the disclosure of an individual's personal data.

However, companies are not liable for disclosures made for purposes mandated by law, such as for criminal investigations.

Disclosures made for the purposes mandated by law is also regulated under Article 23 of MOCI Regulation 20. An electronic system provider is obliged to provide personal data contained in an electronic system based on a valid request from a law enforcement agency.

17. Are data subjects notified if law enforcement accesses their data?

Prevailing regulations are silent on whether data subjects are notified if law enforcement accesses their data.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

There is a draft bill on wiretapping which is currently being deliberated in the House of Representatives. There are opposing views on whether or not wiretapping should be done only with a court order. Arguments have been made claiming that court order processes are lengthy and could undermine the efficiency of investigations. On the other hand, there are arguments stating that court orders are necessary to prevent the abuse of surveillance powers.

According to Article 2 of MOCI Regulation 20, the protection of personal data in an electronic system encompasses protection towards obtaining, collecting, processing, analyzing, storing, announcing, sending and/or distributing and deleting personal data. In conducting those activities, if the personal data is confidential then a written approval from the owner of the personal data is required and/or must be conducted based on the prevailing laws and regulations. Specifically for obtaining and collecting personal data, it must be limited towards relevant information according to its purposes and must be accurately conducted. Also, according to Article 20 of MOCI Regulation 20, the owner of personal data may submit a request to delete specific data of an individual owned by him based on the prevailing laws and regulations.

Article 26 of the EIT Law provides a “right to be forgotten”. This article provides that an electronic system administrator is obliged to delete electronic information and/or documents that are not relevant based on the request of the relevant person through a court order. The electronic system administrator is also obliged to provide mechanism

for the deletion of electronic information and/or documents that are no longer relevant.

Ireland

John Cahir
Dublin
Tel: +353 1 649 2943
jcahir@algoodbody.com

Alison Quinn
Dublin
Tel: +353 1 649 2461
alquinn@algoodbody.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

No, in respect of certain types of communications.

Interceptions pursuant to the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 may be performed on foot of an authorization issued by the Minister for Justice and Equality. This power of authorization is limited to interception for the purposes of criminal investigations and/or the interests of the security of the State. The term 'interception' applies to postal communications, as well as communications by fixed or mobile phone.

The Irish Government is currently drafting legislative amendments to reform the 1993 Act. The Irish Government proposes to amend the terms 'interception' and 'communication' and to also provide for a definition of 'communication address' in order to reflect the use of modern technology in society i.e. email and the internet. There is also a legislative proposal to include 'Information Society Services' to fall within the scope of those that must comply with an authorization for interception signed by the Minister for Justice and Equality. Examples of 'Information Society Services' include internet referencing services and social media. In total, there is estimated to be 50 amendments made to the 1993 Act. The texts of these legislative amendments have not yet been published.

Criminal Justice (Surveillance) Act, 2009 is not applicable to activities that would constitute an 'interception' within the meaning of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

4. How can intelligence services compel companies to provide access to data?

The Communications (Retention of Data) Act, 2011 (section 6) provides that the police force (An Garda Síochána), the military, the Revenue Commissioners, or the Competition and Consumer Protection Commission may request an electronic communications or telecommunications service provider to disclose the data they hold. This data is not 'content data' but rather data necessary to identify and trace communications (i.e. traffic data).

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, the Criminal Justice (Mutual Assistance) Act 2008 provides a framework for the exchange of information and co-operation with foreign law enforcement agencies.

The Criminal Justice (Mutual Assistance) Act 2008 terminology is to be revised in accordance with any amendments to be made to the1993 Act.

6. Are data subjects notified of surveillance by intelligence services?

Generally not. Where surveillance is conducted pursuant to the Criminal Justice (Surveillance) Act, 2009, the legislation mandates the confidentiality of such surveillance and authorization thereof (section 13).

Section 10 of the 2009 Act does allow the Minister for Justice and Equality to make regulations respecting the disclosure/non-disclosure

to a data subject of the existence of an authorization or approval, though no such regulations have been made as yet.

A court may also order the disclosure of documentation generated from a surveillance operation, save for instances where the security of the State would be compromised, witnesses would be endangered, where the Gardaí may rely on operational privilege, unless disclosure is in the interests of justice (section 15).

If interceptions occur pursuant to the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, section 12 provides that the Minister for Justice and Equality shall put in place arrangements necessary to ensure that the disclosure of the existence of an authorization is kept to a minimum. The Irish Government has proposed amending the 1993 Act to introduce a new offence of "unlawful interception" which will exclude interception for legitimate purposes e.g. law enforcement purposes / purposes of protecting the state.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Both the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 Act and the Criminal Justice (Surveillance) Act, 2009 contain a 'complaints procedure', by which, a person who believes a communication sent to or by him has been intercepted, or a person who believes that they might have been the subject of an authorization for surveillance, may complain to a Complaints Referee. A decision of the Referee is final.

Data subjects also have a right to take an action for the infringement of a constitutional right.

It is also open to an aggrieved data subject to apply for judicial review of a decision taken by a Minister/State body.

It is unclear whether the 1993 Act will be amended in this respect.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No. There is interaction with the Minister for Justice and Equality, as the Minister with authority to authorize an interception.

Surveillance measures are undertaken or disclosure requests are made by the police force, the military, the Revenue Commissioners or the Competition and Consumer Protection Commission but the confidentiality measures contained in the legislation indicate that the sharing of information does not occur unless it is deemed necessary under the legislation.

The Communications (Retention of Data) Act, 2011 (section 9) obliges a relevant body which makes a disclosure request to prepare a statistics report, which is shared with the Minister for Justice and Equality, the Minister for Defence and the Minister for Finance, depending on the body preparing the report.

An annual State report, which consolidates the information in any reports prepared throughout the year is then submitted to the European Commission.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

In 1982, the Minister for Justice ordered the tapping of a number of journalists' phones. In the subsequent action, Kennedy v Ireland

[1987] IR 587, the High Court held that privacy is a constitutional right of the citizen and that right included the right to have private telephone conversations, without deliberate and unjustified intrusion.

Herrity v Associated Newspapers [2009] 1 IR 316 is a High Court case wherein a newspaper published a number of articles concerning the plaintiff, some of which contained information obtained from the interference with the plaintiff's phone line. This was found to be a breach of her constitutional privacy right and aggravated damages were awarded as a result.

In the case of DPP v Dillon [2002] 4 IR 501, a criminal conviction was quashed on appeal, as the Court found that the applicant had been convicted on foot of evidence obtained by the unlawful interception of a phone call.

11. Do law enforcement authorities need court orders to intercept communications?

No, in respect of certain types of communications. Interceptions pursuant to the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 may be performed on foot of an authorization issued by the Minister for Justice and Equality, subject to satisfying the conditions therein. Such an authorization may only cover postal communications or communications by fixed or mobile phone.

As noted above the meaning of the terms 'interception' and communication' in the 1993 Act are to be amended.

12. How can law enforcement authorities compel companies to provide access to data?

The Communications (Retention of Data) Act, 2011 (section 6) provides that the police force (An Garda Síochána), the military, the Revenue Commissioners, or the Competition and Consumer Protection Commission may request an electronic communications or telecommunications service provider to disclose the data they hold.

This data is not 'content data' but rather data necessary to identify and trace communications.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

The obligation on service providers to retain and disclose data pursuant to the Communications (Retention of Data) Act, 2011 is a mandatory one. The 2011 Act does not provide a mechanism for challenging these obligations.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Statutory: An individual may complain to the Data Protection Commissioner, who may prosecute the offending entity. An individual also has the right to take a direct civil suit against the offending entity for breach of the duty of care owed.

Constitutional: A constitutional right of privacy also exists, which may be enforced by way of an action in the Courts. Herrity v Associated Newspapers confirmed that an action to enforce this right is not confined to an action against the State or State-bodies – it may be taken against private natural and/or legal persons too.

Article 8 of the European Convention on Human Rights also confers upon individuals a right to respect for private and family life, their home and their correspondence.

Article 7 of the EU Charter of Fundamental Rights echoes this, by stating that everyone has the right to respect for their private and family life, their home and communications.

Article 11 of the draft Regulation on Privacy and Electronic Communications 2017/0003 provides that EU law or Member State Law (that is Irish law) can restrict the right of persons to have

electronic communications (electronic communications data and electronic communications metadata) remain confidential and can restrict the right against any interference with electronic communication's provided such restriction is in the general public interest, is a necessary appropriate and proportionate measure in a democratic society and respects the essence of the fundamental rights and freedoms. Activities by competent authorities required for the purposes of the prevention, investigation, detection of prosecution of crime or public security falls outside the scope of the Privacy and Electronic Communications draft regulation.

Article 22 of the General Data Protection Regulation 2016 / 679 which is to come into effect on 25 May 2018 similarly provides that rights of data subject s in respect of their personal data can be restricted in the interests of national security, defence and public security. Activities by competent authorities for the purposes of the prevention, investigation, detection of prosecution of crime or public security falls outside the scope of the General Data Protection Regulation.

The Irish Government is currently seeking dialogue from industry as to whether or not and amendments should be made to the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 providing for encryption.

Depending on the circumstances, privacy may also be protected by way of an action under the tort of breach of confidence.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

In principle, there is nothing restraining the taking of an action against a U.S. company in Ireland, provided the relevant jurisdictional thresholds are met.

The U.S. Government is however protected from any action by virtue of sovereign immunity, for acts done in a governmental capacity, as

opposed to a commercial capacity. This immunity extends to 'emanations of the State', such as the National Security Agency in the U.S.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes.

Without a valid legal basis for the disclosure, an individual may complain to the Data Protection Commissioner, who prosecute the offending entity. An individual also has the right to take a direct civil suit against the offending entity for breach of the duty of care owed.

An action for infringement of a constitutional right may also lie, which is actionable against private natural or legal person.

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

There is no single surveillance body in Ireland, but surveillance and interceptions are carried out by the police force (An Garda Síochána), military intelligence, the Revenue Commissioners and certain data retained may also be requested by the above law enforcement authorities.

Israel

Nurit Dagan
Tel Aviv
Tel: +972 3 692 7424
dagan@hfn.co.il

Daniel Reisner
Tel Aviv
Tel: +972 3 692 2884
reisnerd@hfn.co.il

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

4. How can intelligence services compel companies to provide access to data?

Through court orders. However, such issues could also be regulated via licensing or commercial agreements.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes (however the identity of the foreign services is usually undisclosed).

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Probably, yes. Although surveillance permits are not issued by court orders, such permits could still fall within the scope of judicial review.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes. (1) If the surveillance permit (search or data) is issued by the head of the General Security Service, he should notify the Prime Minister, the Attorney General and the Knesset's Security Service's committee on a periodic basis; (2) If the surveillance permit is regarding wiretaps, the Attorney General, the Knesset's joint committee of the Foreign Affairs and Defense Committee and the Constitution, Law and Justice Committee should be notified on a periodic basis.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

The governmental bodies are notified ex-post, and usually do not have an effect on the process, except for specific cases where the Prime Minister, the Minister of Defense or the Attorney General can revoke the issued permit.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Generally, No. However, there have been some cases where human rights organizations have petitioned to disclose the amount of usage of surveillance measures, but have been denied by the court.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Through warrant, in accordance with Section 23 of the Criminal Procedure Ordinance (Arrest and Search) [New Version], 1969 or in accordance with Section 43 of the said Criminal Procedure Ordinance in light of which a judge can order a person to present an object (including computer data) in his/her possession.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

In general, to the extent that individuals did not consent to the sharing of their personal information, they may raise claims against government bodies or companies for infringement of their privacy.

However:

(1) According to Section 18(2) of the Protection of Privacy Law, 1981 ("Privacy Law"), it shall be a good defense in a civil or a criminal proceeding for infringement of privacy, if the infringement was committed in good faith and in circumstances in which the infringer was under a legal obligation to commit it or if the infringement was committed in the lawful pursuit of the infringer's occupation and in the ordinary course of his/her work.

(2) According to Section 19(a) of the Privacy Law, no person shall bear responsibility for infringement of privacy for an act which he/she is empowered to do under law.

(3) According to Section 19(b) of the Privacy Law, a Security Authority or a person employed by it or acting on its behalf will not be liable for infringement of privacy reasonably committed within the scope of their function and for the purpose of carrying them out. “Security Authority” means any of the following: Israeli police, the Intelligence Branch of the General Staff and the Military Police of the Israeli Defense Forces, the General Security Service and the Intelligence and Special Duties Agency.

(4) According to Section 23B(b) of the Privacy Law, a Security Authority shall be entitled to receive or disclose information for the purpose of carrying out its functions, provided that the receipt or disclosure of information is not prohibited by law.

(5) According to Section 23C of the Privacy Law, delivery of information shall be permitted, where it is not prohibited by law or by principles of professional ethics:

(a) among Public Bodies, where one of the following occurs: (i) delivery of the information within the capacity of authorities or functions of the person delivering the information and it is required for purpose of implementing a law or for a purpose within the capacity of the authority or the function of the person delivering or receiving the information; (ii) the delivery of information is to a Public Body which may request such information by law from any other source;

(b) from a Public Body to a government unit or to another state institution, or between aforesaid units or institutions, if delivery of the information is required for the implementation of any law or for a purpose within the capacity of authorities or functions of the person delivering or receiving the information;

However, no information shall be provided as aforesaid which was provided on condition that it shall not be delivered to others.

"Public Body" means (1) a governmental departments and any other state institution, local authority and any other body carrying out public functions under any law; (2) a body designated by the Minister of Justice by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, provided that such order shall prescribe the categories of information and data items which the body may impart and receive.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Please see our response to question 14 above.

17. Are data subjects notified if law enforcement accesses their data?

Generally, no.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Italy

Francesca Gaudino
Milan
Tel: +39 02 76231 452
francesca.gaudino@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

There are two main intelligence services in Italy. The Internal Intelligence and Security Agency (AISI) is responsible for safeguarding national security from threats originating within Italy's borders, and for protecting Italy's political, military, economic, scientific and industrial interests. In particular, AISI collects relevant intelligence, counters espionage and other hostile activities within national borders, counters subversion, criminal and terrorist activity in Italy. By contrast, the External Intelligence and Security Agency (AISE) is responsible for safeguarding national security against threats originating abroad, protecting Italy's political, military, economic, scientific and industrial interests. In particular, the AISE collects relevant intelligence and counters espionage and other hostile activities abroad.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

Both AISI and AISE are responsible for protecting Italian economic and industrial interests. While AISI acts within Italian borders, AISE operates outside Italy. However, please note that their main purpose is to prevent others from conducting industrial espionage.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

According to the ordinary procedure, interception activities require a prior authorization from the relevant Magistrate.

In particular, on the one hand, should interceptions be deemed necessary to monitor whether individuals already subjected to crime-prevention measures persist in their criminal activities, such

interceptions need to be authorized by the Judge of the Preliminary Investigations of the place where they have to be carried out, upon request of the Public Prosecutor of the same place. In any case, the results of such precautionary interception activity can be used only as arguments to support the need of carrying on a criminal investigation, but do lack any value for the purposes of the proceedings.

On the other hand, interceptions can be authorized by the Judge of the Preliminary Investigation in relation to an ongoing criminal investigation, upon request of the Prosecutor in charge of the latter, provided that the following conditions are met:

(i) there is serious evidence supporting the suspicion a crime has been committed, regardless of any specific suspect having been already identified or not;

(ii) the crime at hand either is punished with life sentence or with imprisonment for a period longer than 5 years, or is among the offenses specifically listed in Article 266 of the Italian Criminal Code or in other national laws;

(iii) the interception activity is absolutely necessary for the investigation concerning the above crime to be carried on.

It is to be noted however that, in case of urgency, whether there are reasonable grounds to believe that any delay may seriously jeopardize the investigation, the Public Prosecutor shall immediately order the interception activity, which has to be notified within 24 hours to the competent Judge of the Preliminary Investigations. Within the 48 hours running from the issuing of the order, the Judge shall then decide whether to validate it or not.

The Italian Supreme Court issued a very important decision on 28 April 2016 ruling that, in the context of investigations/prosecution of organized crime, it is lawful to install a “Trojan horse” malware to consent the remote acquisition of communications and data stored on portable electronic devices of individuals located in private locations.

According to the Supreme Court, it is lawful to use such interceptions in proceedings even if the location has not been specifically identified in the judicial authorization and even if no criminal activity was ongoing in said places. The condition is that the Judge adequately reasons its order to authorize the interception (case no. 6889/2016).

4. How can intelligence services compel companies to provide access to data?

Should the above legal requirements be met, companies cannot in any way escape the obligation to provide access to data in order to facilitate the investigation, on pain of serious consequences − also of criminal relevance (allegation of aiding and abetting, for example) − for all and any individuals within the concerned company may be responsible for the latter not complying with the order.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes.

Cooperation and collaboration with intelligence services of other countries are carried out only for objectives which are common for all countries involved. The fact that cooperation takes place only for common objectives strongly limits said cooperation activities.

6. Are data subjects notified of surveillance by intelligence services?

No.

Interception activities are carried out secretly.

In no case are data subjects notified of surveillance, unless they turn out to be involved in a formal criminal investigation.

In such a case, once the minutes of the interception operations and the related recordings are filed with the office of the competent

Prosecutor together with the authorizing/ordering/validating decrees, the defense counsels of the data subjects under investigation are allowed to listen to the recordings and examine the communication and telematics interactions intercepted, within the term set by the Prosecutor and possibly extended by the Judge.

Following the expiration of the above terms, the Judge then orders the conversations and/or the telematics interactions which do not appear to be manifestly relevant for the purposes of the proceedings to be removed from the investigation file and move to strike out the recordings and minutes whose use is forbidden. Having the right to attend such taking out operations, the Prosecutor and the above defense counsels are notified of it at least 24 hours prior to the order.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Generally no.

In no case shall data subjects have the right to court review of interception measures, unless they turn out to be involved in a formal criminal investigation.

In this latter case they are entitled to challenge the compliance of the interception operations with the relevant procedural laws:

(i) during the investigation phase, by filing defensive briefs with the competent Prosecutor's office;

(ii) should the investigation be formally closed and the Prosecutor has requested the Judge for the defendants to be committed for trial, by raising the related objections in front of the Judge of the Preliminary Hearing, before the discussion on the merits is initiated;

(iii) should the case have come to trial, by raising the related objections before the Court competent for the trial, before the discussion on the merits is initiated.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

According to the ordinary procedure, interception activities require a prior authorization from the relevant Magistrate.

In particular, should interceptions be deemed necessary to monitor whether individuals already subjected to crime-prevention measures persist in their criminal activities, such interceptions need to be authorized by the Judge of the Preliminary Investigations of the place where they have to be carried out, upon request of the Public Prosecutor of the same place. In any case, the results of such

precautionary interception activity can be used only as argumentations to support the need of carrying on a criminal investigation, but do lack any value for the purposes of the proceedings.

On the other hand, interceptions can be authorized by the Judge of the Preliminary Investigation in relation to an ongoing criminal investigation, upon request of the Prosecutor in charge of the latter, provided that the following conditions are met:

(i) there is serious evidence supporting the suspicion that a crime has been committed, regardless of the identification of a suspect;

(ii) the crime is punishable with life sentence or with imprisonment for a period longer than 5 years, or is among the offenses specifically listed in Article 266 of the Italian Criminal Code or in other national laws;

(iii) the interception activity is absolutely necessary for the investigation concerning the above crime to be carried on.

It is to be noted however that, in case of urgency, whether there are reasonable grounds to believe that any delay may seriously jeopardize the investigation, the Public Prosecutor shall immediately order the interception activity, which has to be notified within 24 hours to the competent Judge of the Preliminary Investigations. Within 48 hours from the issuance of the order, the Judge shall then decide whether to validate it or not.

12. How can law enforcement authorities compel companies to provide access to data?

Should the legal requirements be met, companies cannot in any way escape the obligation to provide personal data to law enforcement authorities in order to facilitate the investigation. Non-compliance may result to serious consequences. On that basis, individuals within the concerned company may be held responsible for non-compliance.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

No.

Should the legal requirements be met, companies cannot in any way escape the obligation to provide personal data to law enforcement authorities in order to facilitate the investigation. Non-compliance may result to serious consequences. On that basis, individuals within the concerned company may be held responsible for non-compliance.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

According to Article 2 of the Italian Constitution, Italy "recognizes and guarantees the inviolable rights of the person, both as an individual and in the social groups where human personality is expressed". The right to respect for private life is included among said inviolable rights.

Furthermore, Article 5 recognized the inviolability of the personal domicile and Article 14 states the confidentiality principle for correspondence and every other form of communication. Restriction or limitation of these inviolable rights can only be imposed by judicial decision stating the reasons and in accordance with the guarantees provided by the law.

Article 1 of the Italian Data Protection Code (Legislative Decree No. 196/2003) states that everyone has the right to protection of his/her personal data. According to Article 7, data subjects have the right, among others, to object, on legitimate grounds, to the processing of their personal data, to obtain the deletion, anonymisation or blocking of data that has been processed unlawfully. Article 13 states that, before the collection starts, data subjects must be informed of the: (i) source of personal data, (ii) purpose and method of the processing, (iii) logic applied to the processing, (iv) identification of the data

controller, data processor and data controller's representative (if any), (v) entities and subjects to whom the personal data can be communicated.

In order to enforce the above mentioned rights, data subjects may start a civil proceeding before the judicial authority to obtain compensation for damage suffered as a result of an unlawful processing of their data or they may apply before the Italian Data Protection Authority to present a circumstantial claim in order to report an infringement of the relevant Data Protection Code's provisions or to directly enforce the rights set under Article 7 of the Code.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

According to Article 5 of the Italian Data Protection Code, the provisions of the Code shall apply to the processing of personal data, including data held abroad, where the processing is performed by any entity established in the State's territory or by an entity established in the territory of a country outside the European Union, where said entity makes use in connection with the processing of equipment, whether electronic or otherwise, situated in the State's territory, unless such equipment is used only for purposes of transit through the territory of the European Union.

Therefore, it seems likely that data subject may enforce their privacy rights against U.S. companies, whether one or more of their subsidiaries are located in Italy, or against U.S. government whether it adopts equipment situated in Italy to collect and process data.

Please note that, on 6 October 2015, the Court of Justice of the European Union issued its judgment in case C-362/14 "Maximillian Schrems v Data Protection Commissioner" and declared Commission decision 2000/520/EC on the adequacy of the EU-US Safe Harbor arrangement invalid.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes.

Please note that processing of personal data includes the communication of personal data. In particular, the latter means disclosing personal data to one or more identified entities other than the data subject, the data processor and persons in charge of the processing in any form whatsoever.

Following the above, it should be noted that according to Article 23 of the Italian Data Protection Code, processing of personal data by private entities shall only be allowed if the data subject gives his/her express consent. Moreover, the data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information listed in Answer 14.

Consequently, the processing of personal data carried out in breach of the above mentioned provision could lead to administrative pecuniary sanctions of up to 120,000 Euros for companies. The fine may be increased up to four times when deemed appropriate in consideration of the company's economic capacity. Moreover, in the worst case, said failure could lead to a criminal sanction according Article 167 of the Code.

17. Are data subjects notified if law enforcement accesses their data?

No.

Interception activities are carried out secretly.

In no case shall data subjects be notified of surveillance, unless they turn out to be involved in a formal criminal investigation.

In such a case, once the minutes of the interception operations and the related recordings are filed with the office of the competent Prosecutor together with the authorizing/ordering/validating decrees, the defense counsels of the data subjects under investigation are allowed to listen to the recordings and examine the communication and telematics interactions intercepted, within the term set by the Prosecutor and possibly extended by the Judge.

Following the expiration of the above terms, the Judge shall order the conversations and/or the telematic interactions which do not appear to be manifestly relevant for the purposes of the proceedings to be removed from the investigation file, and shall move to strike out the recordings and the minutes whose use is forbidden out. Having the right to attend such taking out operations, the Prosecutor and the above defense counsels are notified of it at least 24 hours prior to the order.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

A draft law on the reform of the Italian Criminal Procedure Code is currently being discussed in the Senate and it is the latest attempt to regulate the use of malware to perform interceptions in the course of criminal investigations.

Japan

Daisuke Tatsuno
Tokyo
Tel: +813 6271 9479
Daisuke.Tatsuno@bakermckenzie.com

Kensaku Takase
Tokyo
Tel: +813 6271 9752
Kensaku.Takase@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

No.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Only law enforcement officers may seek warrant from courts to intercept calls and other communications.

4. How can intelligence services compel companies to provide access to data?

Not applicable.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes. The National Security Council of Japan exchange information with other services, including the US NSC.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

No.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

None.

11. Do law enforcement authorities need court orders to intercept communications?

Yes. Under the Act on Wiretapping for Criminal Investigation, local law enforcement authorities can request telecommunication business operators to connect equipment for purposes of intercepting communications or otherwise cooperate in implementing interception of communications. In such case, telecommunication business operators must not refuse to do so without just cause. However, such interception can only be implemented with a warrant issued by court in respect of specific crimes such as drug crimes, organized crime, etc. Further, the Act does not require telecommunication business operators to establish connection with local law enforcement authorities on a daily basis.

12. How can law enforcement authorities compel companies to provide access to data?

Through the warrant issued by the court.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against government: State Redress Act: damages

Against companies: tort (Civil Code): damages

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Yes, under the State Redress Act and the Civil Act.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes.

17. Are data subjects notified if law enforcement accesses their data?

Yes, the data subjects whose calls or communications are wiretapped are notified.

Luxembourg

Laurent Fessmann
Luxembourg
Tel: +352 261844 205
laurent.fessmann@bakermckenzie.com

Amaury-Maxence Bagot
Luxembourg
Tel: +352 261844 288
salome.steinberger@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Intelligence services may operate surveillance programs to protect national security. We are, however, not aware of whether they are currently operating such programs.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

One of the aims of the intelligence service is to protect the private economic actors against threats of industrial or commercial espionage, always using the least intrusive means, proportionate to the aim to be achieved.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

No, the interception of calls, emails, or other communications should result from a decision of a Comity (the "Comity") composed of members of the government, with the assent of a special commission (the "Special Commission") composed of the President of the Superior Court of Justice, the President of the Administrative Court and the President of the District Court. In case of emergency, a Minister can order such measures himself, but has to seize the Special Commission and the Comity as soon as possible.

4. How can intelligence services compel companies to provide access to data?

The director of the intelligence services may, by written notice, ask entities to provide information which it needs for the exercise of its missions. Exceptionally, when all other means fail, and in cases of emergency, the Comity, with the assent of the Special Commission may compel banks and financial institutions to provide access to their data. In case of threat to terrorism, and if all other means fail, it is possible to provide access to private property to collect information.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, the principle of the international cooperation is provided by article 9(4) of the law of 5 July 2016, as amended, on the organization of the State intelligence service.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

No, except when such surveillance measures are taken in violation of the 2002 law on data protection, as amended.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes.

The activities of the intelligence service is subject to the control of a parliamentary commission. Surveillance measures are also subject to the assent of the Special Commission.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Ex post: regarding the control of the parliamentary commission.

Ex ante regarding the Special Commission.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes Historically, there have been doubts regarding the technological and operational means deployed by the intelligence services. This led to the creation of the Parliamentary Commission in 2013.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Law enforcement authorities may compel companies to provide access to data when such data is necessary for the exercise of their public duty, or when it is legitimate to do so, provided that this does not infringe the laws on the protection of personal data nor the mission of the National Commission for such data protection.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes they can challenge such orders, for example if the personal data is contained in documents covered by professional secrecy.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Individuals may only benefit from privacy rights if the personal data has been shared in violation of the rules provided by the privacy and data protection legislation. If this is the case, they may notably oppose the processing of their personal data or file a judicial action for

infringement by the government agency or company of the privacy or data protection legislation.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Yes, depending on the specific circumstances of the case, and if there is a violation of their rights.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes. As mentioned in our answer to question 14, companies may be liable if they have disclosed the personal data in violation of the rules provided by the privacy and data protection legislation (e.g. disclosing personal data where they are not legally requested to do so or where no court order has been issued).

17. Are data subjects notified if law enforcement accesses their data?

Not necessarily. Generally the privacy policies of companies contain a general statement providing that the company may disclose personal data to law enforcement authorities where they are obliged to do (e.g. legal obligation, court order).

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Not applicable.

Malaysia

Woo Wei Kwang
Kuala Lumpur
Tel: +603 2298 7898
weikwang.woo@WongPartners.com

Shameen Binti Mohd. Haaziq Pillay
Kuala Lumpur
Tel: +603 2298 7943
shameen.mohd.haaziqPillay@WongPartners.com

1. Do intelligence services operate surveillance programs to protect national security?

We are not aware of any specific surveillance programs conducted by intelligence services. Such information is not made public.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

We are not aware of whether intelligence services are authorized to conduct industrial espionages or further national economic interests. Such information is not made public.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Pursuant to the Security Offences (Special Measures) Act 2012 ("SOA"), a public prosecutor may authorize a police officer or any other person to intercept information if he considers it is likely that the information relates to the commission of a security offence.

However, a police officer the rank of Superintendent of Police or above may intercept communications without a court order in urgent and sudden cases where immediate action is required leaving no moment of deliberation. He must then immediately inform the public prosecutor of his action and he shall then be deemed to have acted under the authorization of the public prosecutor.

4. How can intelligence services compel companies to provide access to data?

Through court orders.

5. Are national intelligence services cooperating and exchanging information with foreign services?

A bilateral cooperation between Malaysia and the U.S. was reported in October 2015 in relation to the exchange of information and intelligence for purposes of combating terrorism, threats on cyber security and trans-border crime. The cooperative tie, which was contained in Directive No. 6 (HSPD-6) was signed by the Malaysian Home Minister and the U.S. Secretary of State on 8 October 2015. However, details relating to the implementation of the information sharing between the U.S. and Malaysia were not publicly shared.

6. Are data subjects notified of surveillance by intelligence services?

No. The Personal Data Protection Act 2010 ("PDPA"), which is the sole privacy law of Malaysia, is not applicable to Federal and State Governments.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

No.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

We are not aware of this.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

None.

11. Do law enforcement authorities need court orders to intercept communications?

Please refer to our response in Section 3 above.

12. How can law enforcement authorities compel companies to provide access to data?

Through court orders.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes, for instance when the documents are privileged.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Individuals do not have privacy rights pursuant to the PDPA as against government agencies.

Companies may only disclose personal data of individuals without their consent where it is pursuant to an obligation on their part which is conferred by law.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Companies would not be specifically liable to data subjects, but may be prosecuted pursuant to the PDPA.

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Not applicable.

Mexico

Sergio Legorreta-Gonzalez
Mexico City
Tel: +52 55 5279 2954
sergio.legorreta-gonzalez@bakermckenzie.com

Carlos Vela-Trevino
Mexico City
Tel: +52 55 5279 2911
carlos.vela-trevino@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes, the National Security Law (the Law) provides that the National Center for Investigation and National Security (CISEN) shall conduct intelligence activities to protect national security.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

Under certain circumstances, the CISEN may conduct surveillance of financial activities if such are deemed to be connected to threats to national security, for example, the financing of terrorism.

Also, during the investigation of financial crimes, authorities may request the intervention and monitoring of communications by telecommunications operators and application service providers.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

4. How can intelligence services compel companies to provide access to data?

The Federal Telecommunications and Broadcasting Law, the National Security Law and the Guidelines for Collaboration with Security and Justice provide obligations to telecommunications operators, resellers and application service providers to collaborate with authorities. Penalties are imposed if companies do not comply with requests.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Mexico is a party to several international treaties and inter-governmental agreements related to the investigation and prosecution

of crimes, including for example, the participation of Mexico in Interpol as well as the exchange of information under the inter-governmental agreement for the implementation of the United States Foreign Account Tax Compliance Act.

6. Are data subjects notified of surveillance by intelligence services?

No, notifying data subjects is not a requirement.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Reports by organizations such as Freedom House had, in the past, alerted the existence of illegal surveillance activities in Mexico. A recent report published by R3D, a Mexican advocate organization for digital rights ("*State of Surveillance, Out of Control*", 2016) provides,

for the first time, statistics and details of a thorough investigation on this matter in Mexico. The Report suggests that the vast majority of government surveillance operations carried out in Mexico are conducted illegally, either without judicial orders or by government entities that have no legal ground to carry out surveillance practices. The Report also notes that many of the surveillance operations did not result to the filing of criminal actions by Police authorities; for R3D, this evidence suggests that government used surveillance tools for purposes other than the prevention or prosecution of criminal activities.

11. Do law enforcement authorities need court orders to intercept communications?

Yes, as a general rule, any interception of communications must be authorized by a court order. As an exception, no court orders are required before a real time geo-localization operation, but in limited cases, including when the life or the integrity of an individual is at risk. Even in such cases, the authorities must notify the corresponding court within the next 48 hours after the surveillance action was implemented, for the court to verify that the surveillance measures were applied appropriately.

12. How can law enforcement authorities compel companies to provide access to data?

Please refer to answer in question 4.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes, companies may challenge orders if they believe that it is tantamount to a violation of Constitutional rights. Mexican telecom companies are mandated to report quarterly to the Mexican telecom authority the number of requests for surveillance they had received from law enforcement authorities and such telecom authority is

mandated to have such reports publicly available on the Internet. Likewise, the telecom authority must request from the law enforcement authorities for a report on surveillance activities.

Many application service providers that provide services to individuals located in Mexico, but which operate on the Internet with their infrastructure based abroad and which contract through non-Mexican entities, have routinely declined to provide information to Mexican authorities, based on lack of jurisdiction arguments.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Mexico has an extensive framework that allows data subjects to exercise rights of access, rectification, cancellation and opposition related to their personal data before government agencies and private entities (both individuals and companies).

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes, unless transfer is required by law or requested by competent authorities or by judicial authorities. For example, if data is disclosed to administrative authorities for marketing or electoral purposes.

17. Are data subjects notified if law enforcement accesses their data?

No, there is no requirement for notification.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Not applicable.

Norway

Espen Sandvik
Oslo
Tel: +47 98 29 45 41
esa@adeb.no

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes, as a general rule.

The Criminal Procedure Act empowers the prosecuting authority to intercept communications without court order if there is a great risk that the investigation will suffer if the prosecuting authority must wait for the court order. The decision by the prosecuting authority shall as soon as possible, and no later than 24 hours, be brought before the court for approval.

It is also possible to intercept communications based on the general principle of necessity but this legal basis will only apply to very special cases.

4. How can intelligence services compel companies to provide access to data?

Mainly through court orders.

It is also possible to confiscate evidence pursuant to the Criminal Procedure Act. The affected party may immediately or later bring the confiscation before the court, which shall determine whether it shall be upheld.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, Norwegian intelligence services cooperate and exchange information with services of the Scandinavian countries and others. Norway is also part of the Schengen information system.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

The Parliamentary Control Committee (the "EOS Committee") conducts an external and independent control of whether the surveillance measures of the intelligence services are in accordance with the Norwegian law requirements, especially to ensure that individual persons are not subject to any unlawful surveillance. Furthermore, the Ministry and Parliament are, to our understanding, informed of surveillance measures taken that concern national security issues and/or foreign politics issues.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Generally, the Parliamentary Control Committee receives information ex post. It can, however, demand access to and express its opinion on on-going cases.

As for the Ministry and Parliament, there is no clear practice (this information is not publicly available in all cases). Depending on the case and the national security issues and/or foreign politics issues concerned, they may be notified ex ante or ex post.

As regards the second question, the Ministry (through a King of Council decision) has the power to instruct the prosecuting authority in all matters according to the Criminal Procedure Act, e.g. by instructing the intelligence services not to carry out certain surveillance measures or to withdraw an appeal on the lawfulness of a surveillance measure. It should be underlined that this instruction right has never been used by the Ministry.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes, in the 1990s the Parliament appointed a commission headed by Supreme Court judge Ketil Lund (the “Lund Commission”) to inquire into claims that there had been unlawful surveillance of Norwegian citizens since 1945. The Lund Commission concluded that the national intelligence services had conducted unlawful surveillance of Norwegian citizens since 1945, mostly on persons belonging to the left side of the political spectrum.

Following the report from the Lund Commission, the Parliament passed an Act on temporary access to information on oneself registered by the intelligence services. Persons who had suffered

damage by the unlawful surveillance could apply for damages up to a maximum of NOK 100 000 (around EUR 12 000).

11. Do law enforcement authorities need court orders to intercept communications?

Yes as the principal rule but there are some narrow exceptions from this rule as discussed in question 3 above.

12. How can law enforcement authorities compel companies to provide access to data?

By confiscation, warrants for live interception and location information, court orders for stored communications and/or subpoenas.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes, companies do occasionally challenge court orders to provide personal data to law enforcement authorities or confiscation by the intelligence services.

The Supreme Court has recently heard a case concerning a confiscation of a filmmaker's memory sticks and hard disks, containing footage from a documentary on the Islamic community in Norway. The Supreme Court ruled that the confiscation was unlawful as it violated the right to protection of sources.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

If the transfer of personal data is legal, the individual may (naturally) not seek injunctions, damages etc. against the company or the government agency. Whether the transfer is legal depends on an assessment of the Acts mentioned above (especially the Personal Data Act, The Act on Processing of Information in the Police and the

Prosecuting Authority and the Criminal Procedure Act). With regard to the relationship between the data subject and the company, there may also be an agreement between the parties containing regulations on transfers to third parties. The data subject may therefore (also) be entitled to damages on the grounds that the company has breached the contract between them.

If the company is not authorized to transfer the personal data with the government and the government does not have legal bases for collecting such information, the following apply:

Against government:

The person to whom the personal data may be linked may seek injunctions, damages and attorney fees against the government for an unlawful collection of personal data.

Against companies:

The data subject may as the main rule seek injunctions, damages (see question 16 below) and attorney fees against the company for an unlawful transfer of personal data to the government.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

The Personal Data Act will apply to U.S. companies established in Norway or that make use of equipment in Norway. Norwegian data subjects may assert privacy rights against such companies.

Norwegian data subjects may not assert the Personal Data Act or similar legal bases against the U.S. government, with a possible exception for situations where the U.S. government collects personal data solely for business purposes.

American data subjects may assert privacy rights against Norwegian companies and the Norwegian government under Norwegian laws.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Pursuant to the Personal Data Act companies are liable for any economic loss the data subject has suffered as the result of an unlawful disclosure of personal data to the government.

The company may also be ordered to pay compensation for damage of a non-economic nature (compensation for non-pecuniary damage) as seems reasonable, e.g. if the personal data disclosed are of sensitive nature (religion, sexuality).

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

This subject has attracted considerable political interest in Norway. There is an on-going debate in the Norwegian society on how to combine use of surveillance measures for crime prevention purposes and to protect the privacy of Norwegian citizens.

Paraguay

Nestor Loizaga
Asuncion
Tel: +595 21 318 3117
nloizaga@ferrere.com

Raul Pereira
Asuncion
raPereira@ferrere.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes. Law 5241/14 (the "National Security Law") created the National Security System (the "NSS").

The institutions that operate the NSS are in charge of operating surveillance programs to collect and process information with the aim of producing intelligence.

Please note that, in practice, this law is not being applied at the moment; however, it has been reported that the government wishes to start the operation of both the Secretariat of National Security and the National Security System this year.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes. Article 26 of the National Security Law states that the NSS has to request court orders to obtain information through the interception of communications.

4. How can intelligence services compel companies to provide access to data?

Through court orders.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes.

An agreement signed between INTERPOL and the Southern Common Market ("MERCOSUR") is aiming to streamline global and regional

law enforcement cooperation through an improved police information exchange.

Under the agreement, INTERPOL's global database is linked to MERCOSUR's Security Information Exchange System (SISME), with its new version currently being in a launching phase.

6. Are data subjects notified of surveillance by intelligence services?

No. The National Security Law does require notification of surveillance by intelligence services.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

No. National Security Law does not refer to court reviews of surveillance measures.

Nevertheless, if the information obtained under the National Security Law is used in a judicial procedure, it may be null and void if it was not properly obtained.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes. The NSS has to brief the Paraguayan president and the authorized governmental bodies about useful information related to potential enemies of the peace and national security.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

National Security Law does not foresee the procedure to notify these bodies or if they may object to the measures.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

Yes. The Paraguayan Code for Criminal Procedures states that only a judge may order the interception of communications of a person under investigation.

12. How can law enforcement authorities compel companies to provide access to data?

Through court orders.

Under Article 89 of Law 642/95 ("the Telecommunication Law"), the inviolability of correspondence conducted through telecommunication service is protected, except if authorized by a judicial order.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

No, under Law 4711/12 of Contempt of Court, companies are mandated to comply with the court order.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

The Constitution of Paraguay protects the right to privacy under article 33, while article 36 protects private communications against unlawful interference. Article 135 upholds constitutional remedy of Habeas Data.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes. In Paraguay, the right to privacy is a constitutional right. Companies that disclose data to the government without a court order will be liable.

For example, in a civil procedure, a claim of damages may be filed against the company that disclosed data.

On the other hand, a criminal complaint may be filed against the person who was responsible in in disclosing the information.

17. Are data subjects notified if law enforcement accesses their data?

Generally no, the court order notification will be delivered only to the person or company responsible in providing data.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

In 2001, Paraguay enacted a data protection law which regulates the collection, storage, distribution, publication, modification, destruction, duration and the treatment of personal data contained in public and private databases.

However, the abovementioned law was only designed to protect financial data.

Furthermore, it failed to create a data protection authority.

Peru

Teresa Tovar
Lima
Tel: +51 1 618 8500 Ext. 552
Teresa.tovar@bakermckenzie.com

Viviana Chavez
Lima
Tel: +51 1 618 8500 Ext. 421
Viviana.chavez@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No. National Intelligence aims to produce useful knowledge for taking decision on national security matters. Industrial espionage would be out of the scope of the faculties granted to the Peruvian Intelligence Service (called “DINI”).

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

4. How can intelligence services compel companies to provide access to data?

Through court orders.

5. Are national intelligence services cooperating and exchanging information with foreign services?

We have no information on that regard. However, the legal framework does provide the need of promoting cooperation relationships with intelligence services from another countries.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

There are no provisions on this regard. However, if through surveillance measures constitutional rights are affected, the data subjects can denounce such situation.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No. However, note that DINI's activities are under the supervision and control of the Commission of Intelligence of the Congress, who may access to information regarding surveillance measures taken by the DINI.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Ex ante and ex post. The legal framework provides that the Commission of Intelligence can ask for an annual report regarding the programmed intelligence activities, as well as of the intelligence activities conducted.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes. It is called "DINI Case".

The Intelligence Commission of the Congress has recently enacted two reports that confirm an espionage conducted by the DINI to politicians, journalists and business men. Such report will be

discussed by the plenary of Congress in order to determine which actions should be taken.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Through court orders.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

In virtue of the data protection law, companies could ask law enforcement authorities to indicate the legal basis of the request and/or challenge orders to provide personal data. However, they are not incentivized to do it in order to avoid any sanction for refusal to cooperate with such authorities.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

According to the Data Protection Law, the transfer (and further processing) of personal data to government agencies for the compliance of their functions (within the competences granted by the legal framework) doesn't have to be authorized by the data subjects and its processing has legal basis. Only if the information is not intended for the execution of their functions, the data subject can oppose to such processing of information or can file a claim against the government agency for an illegal processing of information.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

There is no jurisprudence on this regard. However, theoretically, companies should only provide personal data if there is legal basis for that (for example, if the information is necessary for the execution of the government entity's functions). However, to determine that may not be an easy task in many cases and this situation should be considered by the Data Protection Authority at the time of determining any responsibility for the access to such information.

17. Are data subjects notified if law enforcement accesses their data?

The Data Protection Law does not provide the need to do such notification.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Portugal

César Bessa Monteiro
Lisbon
Tel: +351 213 264 747
cesar.bmonteiro@pbbr.pt

César Bessa Monteiro, Jr.
Lisbon
Tel: +351 213 264 747
c.monteiro@pbbr.pt

Ricardo Henriques
Lisbon
Tel: +351 213 264 747
ricardo.henriques@pbbr.pt

1. Do intelligence services operate surveillance programs to protect national security?

Law 30/84 of September 5 (Portuguese Information System Law) does not allow intelligence services to conduct searches, process or disseminate information in violation of the rights, freedoms and guarantees laid down in legislative and constitutional frameworks (e.g. privacy and confidentiality in communications).

Also, the law does not allow intelligence services to exercise powers, practice acts or conduct activities which fall under the jurisdiction of the courts or the police.

In Portugal, the intrusion in the privacy of individuals is only allowed in the course of criminal proceedings and only the criminal police is allowed to conduct surveillance programs regarding crime prevention and detection.

According to Draft Law no 345/XII, Portuguese intelligence services could develop monitoring and surveillance actions in public spaces or in private spaces with public access for the prevention of terrorism, espionage, sabotage and highly organized crime. However, this Law was not enacted by the President and, therefore, it was not published and did not enter into effect.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Pursuant to Law 53/2008 of August 29th (Portuguese Internal Security Law), only the criminal police ("Polícia Judiciária") is allowed to monitor communications, through Court authorization.

4. How can intelligence services compel companies to provide access to data?

The directors, officers and deputy directors of the Portuguese intelligence services have access to information and records, relevant to the pursuit of their powers, which are contained in public entities files.

Public companies and private companies that develop relevant activity in the context of contractual relationship with the Portuguese State, within the jurisdiction of intelligence services, shall collaborate with such intelligence services.

In the context of the criminal investigation, only judicial authorities, assisted by the police, may perform the necessary acts, namely to compel companies to provide data. These acts are driven and developed by the police, subject to the authorization, order or validation by the judicial authority.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Portuguese Internal Security Law establishes that the forces and security services may act beyond Portuguese jurisdiction, by cooperating with bodies and services of foreign States or with international organizations.

Draft Law no 345/XII established that the Portuguese Information System may, in accordance with the guidelines set by the Prime Minister, cooperate with similar organizations and international organizations. However, this Draft law was not enacted, as explained above.

6. Are data subjects notified of surveillance by intelligence services?

Only the criminal police is allowed to conduct surveillance in the context of criminal investigation. Data subjects are not notified of surveillance.

The defendant may, however, analyze the result of the investigation (e.g., recordings or transcripts of communications, etc.) after the end of the investigation to prepare their defence.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Only the criminal police is allowed to conduct surveillance in the context of criminal investigation.

Data subjects may argue that the surveillance measures are null and void and, as such, the evidence obtained is also null and void ("fruit of the poisonous tree").

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Only the criminal police is allowed to conduct surveillance in the context of criminal investigation.

Governmental bodies are not notified of surveillance measures taken by criminal police.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

A recent case tackles the alleged violation by the Portuguese intelligence services of the applicable laws relating to surveillance measures. A former director of the Defense Strategic Information System is being prosecuted for corruption, violation of State secrecy, abuse of power and unlawful access to personal data. The defendant has confessed that he had unlawfully accessed personal data of a journalist. As his defense, he claims that this is a common practice among the intelligence services, even if the Law does not allow it. The Court proceedings are still pending.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Through court orders/authorization.

In situations like terrorism or violent or highly organized crimes, among others, both the Portuguese Criminal Code and the Portuguese Cybercrime Law allow the police to conduct searches without previous authorization from the Court. However, in such cases, the search must be validated by the Court. Also, the police may confiscate data without previous authorization by the Court, during a search or whenever it is urgent or there is danger in delay.

According to Portuguese Cybercrime Law, confiscated computer data which contains personal data must be presented and evaluated by the Court.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Pursuant to Law no 67/98 of October 26 (Portuguese Data Protection Law), individuals may use administrative and jurisdictional resources to ensure compliance with data protection rules. Therefore, individuals may file (i) a complaint with the Portuguese Data Protection Authority; (ii) a criminal complaint if the said sharing is a criminal offence; (iii) an injunction to prevent or to immediately stop the said sharing or (iv) a claim based on civil liability, for the damages suffered.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

The Portuguese Data Protection Law does not distinguish data subjects according to their nationality. Such Law applies when: (i) the data controller is located on Portuguese territory; (ii) the processing of the data occurs outside the national territory, in a place where Portuguese law applies; (iii) the data controller, who is not established within the European Union, uses equipment for processing located on Portuguese territory. Therefore, the Portuguese Data Protection Law will apply to all the personal data processing falling within the scope of the Law, regardless of the nationality of the data subject.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Generally, yes. Pursuant to Portuguese Data Protection Law, any person who has suffered damage as a result of unlawful processing of data is entitled to receive compensation from the controller for the damage suffered, unless the controller proves that he is not responsible for the event giving rise to the damage.

17. Are data subjects notified if law enforcement accesses their data?

Generally, yes. Portuguese Data Protection Law establishes a duty of information of the data subject whenever his/her data is collected, registered or communicated to third parties. However, this duty may be waived through legal provision or decision of the Portuguese Data Protection Authority for reasons of national security or prevention or investigation of a crime.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Russia

Edward Bekeschenko
Moscow
Tel: +7 495 787 2700
ed.bekeschenko
@bakermckenzie.com

Evgeny Reyzman
Moscow
Tel: +7 495 787 2700
evgeny.reyzman
@bakermckenzie.com

Vadim Perevalov
Moscow
Tel: +7 495 787 2700
vadim.perevalov
@bakermckenzie.com

Alexander Monin
Moscow
Tel: +7 495 787 2700
alexander.monin
@bakermckenzie.com

Roman Butenko
Moscow
Tel: +7 727 330 0500
roman.butenko
@bakermckenzie.com

Oleg Blinov
Moscow
Tel: +7 495 787 2700
oleg.blinov@bakermckenzie.com

Oleg Tkachenko
Moscow
Tel: +7 495 787 2700
oleg.tkachenko
@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

Yes.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes, intelligence services that intervene with an individual's constitutional right to privacy of communications require a court order.

In urgent matters involving serious crimes, the authorities may undertake surveillance actions without a court order, but are obliged to notify a judge within 24 hours after an interception is initiated. If within 48 hours, no court decision is issued the interception must be terminated.

Starting from 1 July 2018, telecom providers and certain Internet communication services (such as instant messengers) will be required to retain and store on Russian territory contents of all communications by virtue of generally applicable statutory requirements rather than court orders. Still, court orders will be required for law enforcement authorities in order to access such data.

4. How can intelligence services compel companies to provide access to data?

All telecom providers (including both telephone and Internet access providers) are required to implement certain equipment and software selected by intelligence services for interception of data, which is one of their telecom licensing conditions. Such equipment/software enables intelligence services to remotely perform interception without any involvement of telecom providers. Starting from July 1, 2018,

telecom providers will also be required to retain and store contents of all communications within Russian territory.

Internet communication services (such as instant messengers) are also required to retain and store metadata on all communications of their Russian users in the Russian territory. Starting from July 1, 2018, Internet communication services providers will also be required to retain and store contents of all communications of their Russian users in the Russian territory.

In certain situations, when authorized to request data, authorities within criminal investigation may also issue binding orders to companies to produce documents/information. Failure to comply with orders may result in administrative prosecution of a relevant company and its officers in the form of fines.

Alternatively, criminal investigation authorities are also authorized to order and conduct searches and seizures at companies' premises to obtain certain documents or electronic data.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes.

Moreover, A person who is in possession of the facts of the operational-search (detective) measures to which he or she was

subjected and whose guilt has not been proved in accordance with the procedure prescribed by law, that is, he or she has not been charged or charges have been dropped on the ground that the fact of the alleged offence, or the criminal nature of the act was not proved, is entitled to receive information of the data collected in the course of the detective activities, to the extent compatible with the requirements of operational confidentiality and excluding the data that could lead to the disclosure of state secrets.

However, on December 4, 2015, the Grand Chamber of the European Court of Human Rights concluded that "that Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications. In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity. Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference. The domestic law permits automatic storage of clearly irrelevant data and is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial. The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society". The supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions." (Roman Zakharov v. Russia).

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of

(individual) surveillance measures taken by intelligence services?

No.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes, some of the cases were considered by Russian courts (e.g., cases re. falsification of evidence of surveillance).

The consequences of the recent ECHR decision in Zakharov v. Russia are still not clear. Probably, the conclusions of ECHR will be ignored in practice.

11. Do law enforcement authorities need court orders to intercept communications?

Please see answer to Question 3.

12. How can law enforcement authorities compel companies to provide access to data?

Please see answer to Question 4.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes, they can. In certain cases, companies successfully challenge administrative sanctions imposed on them by law enforcement

authorities for refusal to provide information that contains personal data. Such claims are usually satisfied given that the respondent is not empowered by law to conduct surveillance and/or similar procedures.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Individuals have the right to demand from government agencies that the data obtained by agencies be processed only in cases and within the procedure stipulated by law (e.g., for criminal investigation-related matters). Individuals may potentially challenge the orders to companies issued by government agencies to disclose such individuals' personal data.

Individuals may also (a) initiate civil cases against companies or (b) file complaints against companies with the national data protection authority, requesting to prohibit disclosure of their personal data to government agencies in violation of the established procedure.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Theoretically data subjects have the right to claim damages and moral harm for wrongful disclosure of his/her personal data to the government without sufficient legal basis. However, we have found no cases law supporting this.

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Singapore

Ken Chia
Singapore
Tel: +65 6434 2558
ken.chia@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No, the legal basis for surveillance is focused on law enforcement and national security.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

No.

4. How can intelligence services compel companies to provide access to data?

Through powers granted via various legislation, such as the *Criminal Procedure Code, Computer Misuse and Cybersecurity Act, Internal Security Act and Sedition Act.*

5. Are national intelligence services cooperating and exchanging information with foreign services?

There is no publicly available or verified information that Singapore national intelligence services cooperate and exchange information with any foreign intelligence services.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

No.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

N/A

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

No.

12. How can law enforcement authorities compel companies to provide access to data?

Through a production order.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

While challenges are possible, we are unaware of any high profile cases involving the same.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against government: None.

Against companies: Certain protections under the *Personal Data Protection Act 2012*, although please note that exceptions exist in relation to sharing of personal data with the government, in particular for purposes of an investigation or proceeding.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

N/A

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Generally, yes, although please note there are broad exceptions to the disclosure of personal data to the government. Further, there are currently no examples given the nascent nature of the Singapore *Personal Data Protection Act 2012.*

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No, other than the fact that Singapore intelligence services and law enforcements have broad powers to conduct surveillance.

South Africa

Darryl Bernstein
Johannesburg
Tel: +27 0 11 911 4367
darryl.bernstein@bakermckenzie.com

Widaad Ebrahim
Johannesburg
Tel: +27 0 11 911 4384
widaad.ebrahim@bakermckenzie.com

Deepa Ramjee
Johannesburg
Tel: +27 0 11 911 4368
deepa.ramjee@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes. Intelligence services are able to conduct surveillance if, inter alia, there are reasonable grounds to believe that the gathering of information concerning an actual or potential threat to national security, is necessary. Surveillance of this nature is regulated under the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (RICA) and (subject to limited exceptions) generally requires a prior court order.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

RICA does, however, provide for certain exceptions which allow for the lawful interception of communications by law enforcement officials (including intelligence services, police services and the military) without a court order. These include:

(a) when a law enforcement officer is a party to the communication and satisfied that there are reasonable grounds to believe that the interception of a communication of another party to the communication is necessary on a ground referred to in section 16(5)(a) of RICA, unless such communication is intercepted by such law enforcement officer for purposes of committing an offence;

(b) when a law enforcement officer is, inter alia, one of the parties to the communication and who has given prior consent in writing to such interception and the interception of such direct or indirect communication is necessary on a ground referred to in section

16(5)(a) of RICA, unless such communication is intercepted by such law enforcement officer for purposes of committing an offence;

(c) if any law enforcement officer is satisfied that there are reasonable grounds to believe that a party to the communication has, inter alia, caused, or may cause, the infliction of serious bodily harm to another person;

(d) for purposes of determining a location in case of emergency; or

(e) when a law enforcement officer is authorised by certain other legislation.

4. How can intelligence services compel companies to provide access to data?

Through court (interception) orders[24].

5. Are national intelligence services cooperating and exchanging information with foreign services?

From a South African perspective, this information is generally not publicly available, apart from specific incidents reported in the media. RICA does, however, contemplate the issuing of interception directions to assist foreign competent authorities, in connection with, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, if doing so is in:

[24] There are three types:

- an interception direction, which authorises the interception, at any place in South Africa, of any communication in the course of its occurrence or transmission, and includes an oral interception direction;
- real-time communication-related direction, which directs a telecommunication service provider to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available, and includes an oral real-time direction; or

archived communication-related direction, which directs a telecommunication service provider to provide archived communication-related information in respect of a customer.

a) accordance with an international mutual assistance agreement; or

b) the interests of the Republic's international relations or obligations[25].

6. Are data subjects notified of surveillance by intelligence services?

No.

Section 16(7)(a) of RICA clearly states that an application for an interception order must be considered and granted without any notice to the data subject and without affording the data subject a hearing. There is also no requirement to inform a data subject of the existence of interception direction once the investigations are concluded, or if the application was rejected by the designated judge.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No, not of individual surveillance measures.

[25] The Financial Intelligence Centre Act, 2001 (**FICA**) also establishes a Financial Intelligence Centre (**Centre**) and a Money Laundering Council in order to combat money laundering activities. An entity outside South Africa performing similar functions to the Centre, may, at the initiative of the Centre or on written request, obtain information which the Centre reasonably believes is relevant to the identification of the proceeds of unlawful activities or the combating of money laundering or financing of terrorist and related activities or similar offences in the country in which that entity is established.

Interception centers carrying out interception orders are required to provide an annual report to the Minister of State Security and Parliament's Joint Standing Committee on Intelligence (Committee), reporting on aggregated statistics regarding its functions. These statistics are then tabled (in a report on the activities of the Committee) in Parliament in May of each year.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

The Committee is notified ex post facto. Since the Committee performs oversight functions, which include the administration, financial management and expenditure of services in relation to intelligence and counter-intelligence functions, the Committee can raise objections to the measures.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes.

In October 2005, the National Intelligence Agency was alleged to have spied on African National Congress member, Saki Macozoma. Three senior officials, including the-then director-general, were suspended following an investigation by the Inspector-General of Intelligence.

In January 2017, a South African newspaper reported that although only 826 interception orders had been granted between 2006 and February 2010, three million interceptions had been carried out during the same period (as contained in the 2009/10 Committee's annual report), ostensibly, without the necessary authorization. To date, there has been no verification of the figures used in the Committee's 2009/10 annual report.

We are not aware of any other publicized cases.

11. Do law enforcement authorities need court orders to intercept communications?

Yes. See 3 above.

12. How can law enforcement authorities compel companies to provide access to data?

By obtaining an interception direction. Discussed in answer to 4 above.

Where necessary, law enforcement officials may also apply for an entry warrant which would give them access to premises for the purpose of intercepting communications.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes. RICA confirms that a telecommunications service provider in receipt of a interception direction, may apply for an amendment or cancellation of the direction on the ground that their assistance cannot be performed in a timely manner.

In practice, on receipt of a court order, a company or telecommunications service provider, will likely provide access to information sought.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Section 14 of the Constitution of the Republic of South Africa protects the right to privacy. This right includes the right not to be searched or have one's property searched. It also includes the right not to have the privacy of one's communications infringed.

Potential remedies against government agencies or relevant companies, include:

(a) the actio iniuriarum (similar to tort) for the recovery of actual damages suffered[26], or injunctive relief.

(b) statutory relief. Under RICA, if interception is unauthorized, it is an offence and liability could include a fine not exceeding ZAR 2 million (approximately, USD 136 000) or imprisonment for a period not exceeding 10 years.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Generally, yes.

There is technical legal risk but, historically, there has been no uniform approach, as claimants often find it difficult to demonstrate the measure of harm suffered, pursuant to the disclosure.

17. Are data subjects notified if law enforcement accesses their data?

No. See 6 above.

[26] A Claimant will have to prove i. conduct (act/omission) ii. harm iii. fault (intention/negligence) iv. causation v. wrongfulness (unlawfulness).

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

South Africa has also recently enacted the Protection of Personal Information Act, 2013. While the Act, generally requires that data subjects be notified of any processing (or disclosure) of their personal information, "notification" is not necessary if disclosure is linked to the identification of financing of terrorist and related activities, defence or public safety. The precise interplay between this Act, when it comes into force, and the RICA, in relation to the disclosure of information to law enforcement authorities, remains to be seen.

RICA is the only enforcement measure for surveillance from a South African perspective. The potential abuse of this regulation is a "hot-topic" in South Africa, and calls for legislative reform of surveillance laws are rife.

South Korea

Boseong Kim
Seoul
Tel: +82 2 721 4130
boskim@kcllaw.com

Junghwa Lee
Seoul Tel: +82 2 721 4147
jhlee@kcllaw.com

Mike Shin
Seoul
Tel: +82 2 721 4140
mikeshin@kcllaw.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

Yes.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

4. How can intelligence services compel companies to provide access to data?

A court approval must be obtained, except where access to data is urgent due to a conspiracy which threatens the national security, etc. (in which case, however, an ex post facto court approval must be obtained).

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes.

6. Are data subjects notified of surveillance by intelligence services?

Yes. Data subject are notified within 30 days after the close of intelligence services.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Date subjects do not have such right under the Protection of Communications Secrets Act, but may file a claim for damages and/or a criminal action if there is illegal wiretapping.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

The National Assembly may request courts or intelligence service to report on the details of surveillance measures.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Ex ante.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes, illegal wiretapping by the National Intelligence Service has often become an issue.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

A court approval must be obtained.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

No.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Individuals may request government agencies or companies to stop such sharing under the Personal Information Protection Act, but government agencies may refuse such request if necessary to carry out their duties.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes. But it is rare that damages were actually granted.

17. Are data subjects notified if law enforcement accesses their data?

No. But data subjects are notified ex post if law enforcement takes measures that limit communications or is provided information on data subjects' communications.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Discussion about amending the Protection of Communications Secrets act is in progress due to terror threats, so it would be advisable to monitor legal developments on a regular basis.

Spain

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com

Ignacio Vela
Madrid
Phone: +34 91 230 45 09
ignacio.vela@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

The main intelligence service in Spain is the Spanish National Intelligence Center ("SNIC"). Its legal basis are the Act 11/2002, regulating the SNIC ("Act") and the Organic Act regulating a prior judicial control of the NIC ("OL"). One of its functions, as determined by the Act, is to prevent, detect and provide for the neutralization of the activities that endanger, threaten or attack the security of the Spanish State and the stability of its institutions. To perform its functions, the Act recognizes the ability of the NIC to conduct security investigations on individuals and entities.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

Although the SNIC's main objective is of public interest (the SNIC does not work on the interest of private entities), one of its functions set forth by the Act is to collect, assess and interpret information and disseminate the necessary intelligence to protect and promote the political, economic, industrial, commercial and strategic interests of Spain, both inside and outside of Spain.

Therefore, it can not be ruled out that the SNIC can act in favor of national economic interests of Spain although we understand that its main purpose for this function is to prevent others from conducting industrial espionage.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes.

When the investigations of the SNIC imply measures that could affect the secrecy of communications, the OL sets forth that the SNIC shall require authorization from one specific Magistrate of the Spanish

Supreme Court (specially appointed for that purpose every 5 years) provided that the mentioned measures are needed to fulfill the functions assigned to the SNIC by the Act.

The written request of authorization to be submitted by the SNIC to the aforementioned Magistrate shall always contain the following aspects:

(i) specification of the particular measures that are being requested;

(ii) supporting factual grounds of the request, purposes of such request and reasons for the adoption of the measures requested;

(iii) if known, identification of the concerned individual(s) affected by the measure and designation of the place in which the measures shall be implemented;

(iv) duration of the measures requested, which shall not exceed 3 months in case of interception of communications (extendable time limit if necessary).

Afterwards, within 72 hour-terms (or within a 24 hour-terms in case of urgency, if so, it is indicated in the relevant SNIC's request), the Magistrate will deny or authorize the request of the SNIC by adopting a resolution setting out the grounds on which its decision is based that shall contain the aspects above mentioned.

Spanish case law has indicated that the Magistrate is the one in charge of evaluating if the requested measure is needed to fulfil the functions of the SNIC and to weigh the measure requested against the fundamental right of secrecy of communications.

Additionally, all the actions of the Magistrate regarding the authorization or denial of the communications interceptions requested by the SNIC are classified as top secret by the OL.

4. How can intelligence services compel companies to provide access to data?

Although neither the Act or the OL sets forth a general obligation for companies to provide access to data when requested by the SNIC, article 5 of the Act establishes that the SNIC may request the necessary collaboration from public and private institutions in order to conduct its security investigations.

In addition, as long as the SNIC shall obtain the authorization of the Magistrate for communications interception there will be a duty to cooperate with justice.

Against this background, the General Telecommunications Act ("GTA") sets forth that telecommunications operators must have in place one or more interfaces through which intercepted electronic communications and information relating to the interception shall be transmitted to the reception centers of communications interception. Moreover, prior to the execution of the authorized communications interception, operators are obliged to facilitate information regarding the services and characteristics of the telecommunications systems used by the persons affected by the communications interceptions along with, if known by the operator, several data (name, national identification number, tax identification code, etc.).

In addition, GTA establishes that telecommunications operators have to facilitate access to any kind of electronic communication, in particular, for those carried out by any means of telephone and data transmission even if they are video communications, audio, exchange messages, files or facsimile transmissions.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Generally, yes.

Although there is no actual evidence that this kind of cooperation is taking place, the Act expressly foresees this possibility establishing,

as one of the functions of the SNIC, the promotion of relationships of cooperation and collaboration with intelligence services of other countries or international organizations in order to meets its objectives more efficiently.

6. Are data subjects notified of surveillance by intelligence services?

Generally, no.

Even when the surveillance measure has already been implemented and carried out for the achievement of its purpose, instances where data subjects are notified of the surveillance are very rare.

The main reason for this, as clarified by the Spanish Supreme Court, is that the actions of the SNIC can not be considered as judicial acts of investigation. The SNIC does not investigate facts that could constitute criminal acts (as in the context of law enforcement powers' investigations). The objectives of the SNIC are different from those in a criminal proceeding. The SNIC aims to provide the Government with information for a whole range of functions that are not related at all with the investigation of a criminal act but serve to justify the communications interception.

Consequently, surveillance measures adopted by the SNIC are not usually used as a real means of evidence for the purpose of a criminal proceeding and therefore they are not usually disclosed. Additionally, as mentioned in question 3, the actions of the Magistrate are deemed top secret, which would mean that in order to notify the interception measures it would be necessary to first have it declassified.

In conclusion, the only possibility through which the subject affected can be notified of a certain interception measure would be in case that the measures adopted by the SNIC are used as a means of evidence in the correspondence judicial proceeding and have been previously declassified (both exceptional situations).

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Generally, no.

As the activities of the SNIC are not considered as judicial acts of investigation, the Spanish Supreme Court has indicated that they are not considered to be under the principle that both parties must be heard and the rights of defense. Therefore, data subjects do not have a right to court review of the measures adopted by the SNIC, being, as indicated by the Spanish Supreme Court, the absence of any challenging possibility part of the very nature of the judicial control system set fort by the OL.

The SNIC activities are subject to the above mentioned judicial control, but such control procedure ends at the very moment of the final authorization by the Magistrate when it has already made its evaluation and weighing.

In this respect, the right to court review of surveillance measures taken by the SNIC has been denied by the Spanish Supreme Court even when the measures of the SNIC are communicated to the Spanish prosecutor's office and eventually arrive at a criminal procedure, although it has not always been the case and it depends on the circumstances of each case (as mentioned, court review of a surveillance measures could be possible if they are used as a means of evidence and have been properly declassified).

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No.

There are three bodies that may have certain control over the SNIC and access to classified information regarding its activities as set forth in the Act:

Government. It shall determine and approve the SNIC's objectives on an annual basis by means of an "Intelligence Directive" that is classified as top secret. Access or notification to the Government of individual surveillance measures taken by the SNIC is not expressly foreseen.

Parliamentary Committee. A specific parliamentary Committee (the same committee which controls public expenses) will be informed of the SNIC's general objectives as approved by the Government. The Parliamentary Committee will also receive the annual report, which evaluates the activities, status and degree of achievement of the objectives set out for the previous year. The content and discussions of this Committee shall remain secret and the documents the members examine shall be returned to the SNIC with no possibility of making any copies.

Government Executive Committee for Intelligence Affairs. This Committee is responsible for proposing to the Prime Minister the annual objectives of the SNIC that should be included in the mentioned "Intelligence Directive" and for monitoring and evaluating the performance of the SNIC's objectives, among other functions. However, the latter does not expressly foresee access or notification of the specific surveillance measures undertaken by the SNIC.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

No.

As mentioned in question 8, the Parliamentary Committee controlling expenses may exercise certain control (ex ante and ex post) in relation to the SNIC's objectives settled by the Government on a year-

on-year basis. However, such control is merely of an informative nature, not implying a right to object to even the aforementioned objectives.

As for the Government, it is foreseen that they shall approve the SNIC's objectives annually. Consequently, the Government shall always have a right to object to these objectives since is the body in charge of approving them. A similar conclusion could be reached regarding the Committee for Intelligence Affairs which is in charge of proposing to the Prime Minister the annual objectives of the SNIC and therefore it could have, in practice, certain right to object to them.

Please note that, again, we are not talking about individual measures conducted by the SNIC but about general objectives pursued by the SNIC.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes.

The most famous case took place during the late 1980s and mid 1990s, when it became known that certain personnel from the former SNIC ("Superior Centre of Defense Information" or "SCDI" then) had been carrying out telephone tapping on numerous personalities (including politicians and King Juan Carlos I) without the corresponding prior judicial authorization. Personnel involved in such illicit telephone tapping were finally convicted by the Supreme Court in 2006 (Sentence 921/2006, "Caso CESID"), while the SCDI then director was acquitted.

It was precisely such scandalous occurrence along with the discovery of microphones in the political wing of ETA's terrorist group's headquarters in Vitoria, which led to establishing a prior judicial

control over the activities of the SNIC by means of the above explained OL.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

The Criminal Procedure Act ("CPA") sets forth the need for prior judicial authorization to intercept communications subject to certain principles: specification (interception shall be related to the investigation of an specific criminal act -it is not possible to authorize interception for the purpose of preventing criminal acts or based on value judgments or mere suspicious); adequacy (it is necessary to define the scope and duration of the interception); exceptionality and necessity (interceptions shall only be agreed when they are no other investigation measures less harmful for fundamental rights) and proportionality (the harm to the secrecy of communications shall not be more that the benefit obtained by adopting the interception).

Pursuant to the CPA, the Courts shall deny or authorize the interception of communications requested within 24 hours by adopting the corresponding resolution that shall have a minimum content (investigated act, duration, identification of the concerned individuals, etc.).

Law enforcement authorities are also obliged to inform the Court of the development and results obtained by the communications interception.

In case of urgency, interception of communications can be authorized by the Ministry of Interior or the Secretary of State for Security in case of criminal acts related to terrorism or armed gangs as an exceptional measure that shall always be confirmed or revoked by the competent Court within 72 hours.

12. How can law enforcement authorities compel companies to provide access to data?

As mentioned in question 4 above, as long as law enforcement authorities shall obtain a prior court order to intercept communications there is a general duty to cooperate with justice. Moreover, as explained above, the GTA sets forth specific obligations for telecommunications operators (have in place interfaces for interceptions, facilitate information regarding the services, etc.)

Additionally, please note that the CPA expressly sets forth an obligation to cooperate with Courts and law enforcement authorities in order to enable the accomplishment of the court order authorizing the communications interception. This obligation is directly addressed to providers of telecommunications services, of access to telecommunication networks or of information society services, and for any person that in any manner contributes to facilitate communications through phone or through any other telematics communication system.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

Companies may challenge court orders to provide personal data to law enforcement authorities. Unlike the case of the SNIC, companies do have access to the court order and can verify if the content complies with the requirements set forth by the CPA and there is a general right for court review of decisions.

However, despite the theoretical possibility of challenging the judicial authorization, the right to review is limited (minimum content, technical implementation, etc.) and companies cannot discuss or make objections to the surveillance measure authorized (i.e. they can not discuss if the judge has evaluated correctly the fundamental right to

secrecy of communications which is a role attributed to the competent court). Additionally, companies are not usually a party in the proceeding where the communications interception will be used as means of evidence which substantially limits the possibility of challenging the authorized communications interception. Consequently, the legality of such judicial authorization to intercept communications is usually challenged by the affected data subject when the interception is submitted as means of evidence in the corresponding criminal proceeding.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Privacy rights of individuals against the government are found in the Spanish Constitution. In particular, in article 18.

Basic right to privacy is laid down in article 18.1:. “The right to honour, to personal and family privacy and to the own image is guaranteed.”

Right to secrecy of communications is laid down in article 18.3: “Secrecy of communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary.” This right is further developed by the GTA and the OL.

Right to protection of personal data is laid down in article 18.4: “The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.” This right is further developed by the Data Protection Act (“DPA”)

Please note that public authorities and citizens, including government agencies and companies, are bound by the Spanish Constitution and all other legal provisions.

Additionally, at a European level, the right to respect for one’s private and family life, his home and his correspondence is settled in article 8

of the European Convention on Human Rights ("ECHR") that has a similar content to article 18 of the Spanish Constitution. In this respect, article 10.2 of the Spanish Constitution expressly mentions that the rights recognized by it must be interpreted in conformity with the Universal Declaration of Human Rights and "the international treaties and agreements on those matters ratified by Spain", which includes the ECHR.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

The territorial scope of the laws regulating the mentioned privacy rights (DPA, GTA, etc.) depend on the application of each regulation. In this respect, neither the nationality nor the habitual residence of data subjects, nor the physical location of the personal data, are decisive for the purpose of determining the application of the relevant regulation.

For example, DPA has as the main criteria for determining its application the location of the establishment of the data controller and, specially, the fact that the processing of personal data is carried out in the context of the activities of the said establishment (although it may also apply if a branch or subsidiary is created in Spain with the intention of promoting the services of the data controller located in a third country and orientates its activity to Spanish customers).

Please note that the EU General Data Protection Regulation ("GDPR" - which will start to apply in May 2018), states that the GDPR will not only apply to the processing of personal data in the context of the activities of an establishment of a controller of a processor in the EU (regardless of whether the processing takes place in the Union or not), but also to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the EU, where the processing activities relate to: (a) the offering of goods or services to such data subjects in the UE or (b) the monitoring of their behavior as far as their behavior takes place within the Union.

On the other hand, GTA has as the main criteria for its application not the place of business of the provider but the place of supply of the services. Therefore, GTA will apply in the moment that a telecommunication service is provided in Spain which would depend on several factors (terms of the agreement, if the client is a consumer, etc.).

Under these circumstances, it seems very likely that data subjects may assert privacy rights against U.S. companies or the U.S. government.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes.

In case companies disclose data to the government without sufficient legal basis, the affected data subjects may claim to the companies the following.

The claim would most likely consist on damages based on either contractual or non-contractual liability depending on the circumstances (if the data subject had or not a contract in place with the corresponding company). Any damages sought by the data subject will depend on its ability to prove both the existence of damages and the casual relationship between the incident (the disclosure of data) and the damages.

Data subjects could initiate a claim based on the violation of their data protection rights. This claim will be initiated before the data protection authority and could end with a fine imposed to the companies. However, in accordance to current applicable regulation, data subjects would not be compensated for the alleged violation of their data privacy rights by the data protection authority (any compensation sought by the data subjects shall follow the damages claim indicated above). From May 2018, the GDPR sets forth the possibility for data

subjects to also receive compensation from the relevant controller or processor for any material or non material damaged suffered as a result of an infringement of the GDPR (i.e. the disclosure of personal data to a third party without legal basis).

Lastly, please note that there is also a possibility of criminal liability (illegal interception of communications is considered a criminal offence), although we consider it unlikely to be upheld given that this kind of criminal offence requires to be done with criminal intent. However, there is also a possibility for legal entities to be criminally liable in the absence of criminal intent. The Spanish Criminal Code expressly states that legal entities may be exempted from criminal liability depending on the circumstances of each case (supervision of the employees, etc.) and the implementation of an organizational and management program that includes supervisory and control measures that are suitable for preventing criminal offences provided that they have been implemented prior to the commission of the offence and meet certain minimum requirements and conditions. Moreover, for the criminal liability of legal entity to arise, it would be necessary that the criminal offence is committed for the direct or indirect benefit of the legal entity.

17. Are data subjects notified if law enforcement accesses their data?

Yes.

Notification of the interception at the moment in which the measure is adopted and implemented is not foreseen. In fact, the CPA sets forth the secretive nature of the request and the potential further actions in relation to the measure.

Notwithstanding the above, provision 588 ter i) of the CPA states that once the secrecy is lifted and the telecommunications interception measure has expired, the parties will have access to the recordings and the transcriptions conducted under the corresponding judicial authorization.

Furthermore, unlike the measures and the information obtained by the SNIC, the measures and the information obtained by law enforcement authorities pursuant to the CPA and the prosecution of certain crimes, does usually arrive as a real means of evidence to a criminal procedure. This means that they are bound by the principle that both parties must be heard and the rights of defense. Therefore, the affected data subject will have knowledge of the measure and will have the possibility of challenging it.

Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang@bakermckenzie.com

Tehsin Wu
Taipei
Tel: +886 2 2715 7327
tehsin.wu@bakermckenzie.com

1. **Do intelligence services operate surveillance programs to protect national security?**

Not to our knowledge.

2. **Are intelligence services authorized to conduct surveillance for an economic purpose?**

No.

3. **Do intelligence services need court orders to intercept calls, emails or other communications?**

Yes.

4. **How can intelligence services compel companies to provide access to data?**

Through court orders.

5. **Are national intelligence services cooperating and exchanging information with foreign services?**

No.

6. **Are data subjects notified of surveillance by intelligence services?**

No.

7. **Do data subjects have a right to court review of surveillance measures taken by intelligence services?**

No.

8. **Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of**

(individual) surveillance measures taken by intelligence services?

No.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Not applicable.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

Yes.

12. How can law enforcement authorities compel companies to provide access to data?

Through court orders.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Legally they can, but we have not seen any claims made.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against government agencies and companies: Personal Data Protection Act, Civil Code: civil, criminal, and administrative liabilities.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Not applicable.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Legally companies are liable, but we have not seen any claims made

17. Are data subjects notified if law enforcement accesses their data?

No if the notice requirement is exempted due to statutory reasons provided in the Personal Data Protection Act.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.

Thailand

Dhiraphol Suwanprateep
Bangkok
Tel: +66 02 636 2000 Ext. 4950
dhiraphol.suwanprateep@bakermckenzie.com

Pattaraphan Paiboon
Bangkok
Tel: +66 02 636 2000 Ext. 4568
pattaraphan.paiboon@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No, unless for the purpose of national security.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

For the purpose of national security, generally no.

4. How can intelligence services compel companies to provide access to data?

Summon information from companies for the purpose of national security.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of

(individual) surveillance measures taken by intelligence services?

Yes.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Yes, either ex ante or ex post.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Not applicable.

11. Do law enforcement authorities need court orders to intercept communications?

Yes, except for the purpose of maintaining public order, good morals, and national security.

12. How can law enforcement authorities compel companies to provide access to data?

Court orders or summons for information from service providers under the Computer Crime Act.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against government: Section 24 of the Official Information Act, B.E. 2540 (1997)

Against companies: Torts

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

No, under the Official Information Act, B.E. 2540 (1997).

Yes, under torts.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Possible under torts.

17. Are data subjects notified if law enforcement accesses their data?

No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Please note that the National Cybersecurity Bill and National Intelligence Bill are under consideration.

Turkey

Hakki Can Yildiz
Istanbul
Tel: +90 212 376 64 54
can.yildiz@esin.av.tr

Can Sozer
Istanbul
Tel: +90 212 376 64 43
can.sozer@esin.av.tr

Hilal Temel
Istanbul
Tel: +90 212 376 64 17
hilal.temel@esin.av.tr

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes, with the exception for emergency cases.

According to Article 6 of Law No. 2937 on the Turkish National Intelligence Agency (Tr. Milli İstihbarat Teşkilatı "NIA"), can intercept communications with a court order. However, in case of an emergency NIA is authorized to intercept communications with the written order of Secretary of NIA or his deputy, without a court order. If an interception to communications is made without a court order, the written order which authorized such interception will be presented to the authorized court for approval within 24 hours. Court decides whether to approve or reject the interception to communications within 24 hours.

In addition, note that Turkey declared a state of emergency on July 20, 2016 after the coup attempt. The state of emergency has been extended as of January 19, 2017 for 90 days.

According to the Decree Law No. 670 on Taking Certain Measures within the Scope of the State of Emergency, all information and documents, including wire-tapped communication should be immediately provided by public and private institutions and organizations in relation to people subject to investigations for the listed crimes, as well as their spouses and children.

4. How can intelligence services compel companies to provide access to data?

By issuing requests.

According to Article 6(b) of Law No. 2937, NIA has the right to compel legal entities and unincorporated associations to provide data and access to data through their systems and archives. If NIA does make such a request, companies cannot evade this request on grounds that the applicable legislation do not authorize such interceptions.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes.

According to Article 6(a) of Law No. 2937, NIA is authorized to communicate, cooperate and apply necessary coordination methods with any and all foreign services.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

As a general principle and as established under Article 125 of the Constitution, all decisions and actions of governmental authorities are subject to judicial review.

According to Article 26 of Law No. 2937, initiation of criminal investigations against intelligence service officials for crimes they allegedly committed in relation to their duty or during completion of their duty, is subject to the Prime Minister's permission.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

No.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Governmental Bodies are notified ex post.

In theory governmental bodies do have a right to object to the measures. According to Article 7 of Law No. 2937 the under secretariat of NIA, who is in charge of running all intelligence operations, is exclusively accountable to the Prime Minister. Relevant governmental bodies can object to the measures by application to Prime Minister. However in practice we are not aware of any such complaints being filed against NIA by governmental bodies.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

There have been many cases where there were suspicions that NIA violated applicable laws relating to surveillance measures. Authorizations for wire-tapping businessmen and journalists were obtained from the court by giving different names for the phone numbers of businessmen and journalists. We are not aware of any cases where the Prime Minister has approved prosecution of NIA officials. In 2014, however, a lawsuit has been filed to administrative court for cancellation of Prime Minister's decision of not allowing initiation of criminal investigation. The administrative court ruled against the Prime Minister's decision and allowed for prosecution.

11. Do law enforcement authorities need court orders to intercept communications?

Yes, with the exception for emergency cases.

According to Article 135 of the Turkish Criminal Procedure Code, in case of emergency, law enforcement authorities can intercept communications upon the decision of a public prosecutor. The public prosecutor, however, must immediately present such decision to the court for approval. Court decides whether to approve or reject the interception to communications within 24 hours.

According to Additional Article 7 of Law No. 2559, in case of emergency, law enforcement authorities can intercept communications upon the decision of Chief of Police or Chief of Intelligence Department. The law enforcement authorities, however, must present such decision to the court for approval within 24 hours. Court decides whether to approve or reject the interception to communications within 24 hours.

12. How can law enforcement authorities compel companies to provide access to data?

According to Article 137 of the Turkish Criminal Procedure Code, within the framework of the decision obtained according to Article 135 of Turkish Criminal Procedure Code (see our answer for Question 11 above), in case the competent enforcement bodies require communication to be detected, investigated or recorded, telecommunications companies are required to immediately comply with any such request.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

According to Article 135 of the Turkish Criminal Procedure Code, companies can object to the court decision allowing the interception of communications by law enforcement authorities. The Court must decide unanimously to cancel the relevant decision.

Please note that interception of communications is allowed only for the crimes listed in the article. Interception of communications can be permitted for a maximum period of two months. The permit period can be extended for an additional month, and for three months in case of an organized crime.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Law No. 6698 on the Protection of Personal Data (the "Data Protection Law") exempts from its reach the following under Article 28:

(i) the processing of personal data for national defense, national security, public security, public order or economic security purposes by the legally authorized public institutions within the scope of preventive, protective and intelligence-related operations.

(ii) the processing of personal data in relation to investigation, prosecution, judgment procedures or execution by judicial authorities or execution offices.

Unless processing falls under the above exemptions, the Data Protection Law will be applicable.

According to Article 5 of the Data Protection Law, the data controllers must obtain explicit consents of data subjects to process their personal data, unless such processing falls under the exemptions exhaustively provided in the Data Protection Law. The exemptions include the following:

(i) processing is specifically designated by the laws, and

(ii) processing is necessary for the data controller to comply with its legal obligations.

If, therefore, the underlying reason for transfer of personal data to government is to comply with the applicable laws, then the processing will be deemed legal. If companies transfer data subjects' personal data to government without any legal grounds, then they have to obtain data subjects' explicit consents with respect to such transfer. Lack of explicit consent may result in individual complaints, and consequently in administrative fines ranging between TRY 5,000 and TRY 1,000,000, as well as criminal penalties.

Data subjects have rights of access to their personal data through application to data controller, however, exercising these rights are subject to above-referred Article 28 of the Data Protection Law.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

As Turkey is not a member of the EU, there is no specific legal mechanism through which Turkish data subjects can assert privacy rights against U.S. companies and the U.S. government.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Companies will be liable to data subjects if they disclose data to the government without the legal grounds stated in the Data Protection Law, as detailed above in answer to Question 14.

Lack of explicit consent may result in individual complaints, and consequently in administrative fines ranging between TRY 5,000 and TRY 1,000,000, as well as criminal penalties.

With regard to criminal penalties, under Article 136 of the Turkish Criminal Code ("TCC"), the illegal transfer, dissemination and

collection of personal data is punishable by imprisonment for one to four years. Private legal entities can be subject to (i) revocation of a license or permit, (ii) confiscation of property or material interests relating to the offence.

17. Are data subjects notified if law enforcement accesses their data?

Generally Yes. In some circumstances, the law requires law enforcement to notify data subjects.

For example, under Article 137 of the Criminal Procedure Law, (i) in case no grounds are found for prosecution as a result of investigation, or (ii) if court rejects the interception to communication conducted in case of emergency upon the decision of a public prosecutor, then the recordings relating to detection and interception are destructed within ten days at the latest under the supervision of public prosecutor. In this case, the data subjects are notified in writing of the reason, scope, time period and outcome of the interception within fifteen days following the end of investigation.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Parliament has been criticized on grounds that it has passed many laws to grant state intelligence units broad powers of surveillance with little accountability or oversight over how they are used. High profile public officials have also become victims of major wiretapping scandals themselves, which have indicated alleged government corruption.

There is little public discussion on the effects of unchecked surveillance in Turkey. Debate on how to protect citizens from unnecessary and unchecked government surveillance has taken place in Turkey, but mostly among civil society groups, rights organizations

and academics. International bodies, including the EU, have so far also reacted to Turkey's stricter surveillance laws.

United Kingdom

Ian Walden
London
Tel: +44 207 9191 247
ian.walden@bakermckenzie.com

Dyan Heward-Mills
London
Tel: +44 207 9191 269
dyann.heward-Mills@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes. In the UK, the key agencies responsible for national security are the Security Services ('MI5') and the Secret Intelligence Services ('MI6). The former has responsibility for domestic counter-intelligence, while the latter is responsible for foreign intelligence. The existence of MI5 was avowed by the government through the Security Service Act 1989 and MI6 by the Intelligence Services Act 1994. Both services have the functions of protecting national security, safeguarding the 'economic well-being of the United Kingdom' and 'the detection and prevention of serious crime'. The agencies are supported by the Government Communications Headquarters ('GCHQ'), which provides signals intelligence. Within the Ministry of Defence, there is also Defence Intelligence, providing strategic defence intelligence to the Ministry and the armed forces.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No. The intelligence services can engage in conduct designed to safeguard the economic well-being of the United Kingdom, but only where relevant to the interests of national security. As such, industrial espionage could only take place for the purpose of protecting national security, not to further national economic interests.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Yes. Either a Ministerial or judicial warrant would be required.

Under the Regulation of Investigatory Powers Act 2000 (RIPA), s. 5, a warrant to intercept must be issued by executive branch in the form of the Secretary of State at the Home Office or the Foreign Office. The current regime will be replaced sometime during 2017 by the Investigatory Powers Act 2016 ('IPA'). Under the IPA, a ministerial

interception warrant would also require approval by a Judicial Commissioner.

The Police and Criminal Evidence Act 1984 ('PACE') allows a court to grant access to material (Schedule 1 and Section 9), which could include stored communications in the course of transmission. Under the Intelligence Services Act 1994 ('ISA'), the Secretary of State can grant a warrant to allow intelligence agencies to interfere with property, which could result in the interception of communications.

4. How can intelligence services compel companies to provide access to data?

RIPA, Part 1, allows for mandatory requests for communications content (Chapter 1) or communications attributes data (Chapter 2) to be made to providers of 'telecommunication services' or those that control telecommunication systems in the UK. The concept of a 'telecommunication service' is very wide and could include any online service provider offering a communications functionality.

5. Are national intelligence services cooperating and exchanging information with foreign services?

The Crime (International Co-Operation) Act 2003 details mechanisms for the mutual provision of evidence. Any request for UK-based evidence by overseas authorities must be sent first to the Secretary of State at the Home Office who may then nominate a court to deal with the request. For requests between EU Member States, the UK will implement Directive 2014/41/EU 'regarding the European Investigation Order in criminal matters' by 22 May 2017. This will provide for cooperation based on the principle of mutual recognition. The UK is also a member of the 'Five Eyes' alliance for joint cooperation in intelligence matters.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes.

An individual has the right in RIPA under s.65 (2)(a) or (d) to bring proceedings, or make a complaint or reference under s.65(2)(b) or (c) to the Investigatory Powers Tribunal.

RIPA also set up the Office of the Interception Commissioner (s.57) who reviews the exercise and performance of the powers and duties granted to persons under RIPA.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes. The Intelligence and Security Committee of Parliament ('ISC') is a statutory committee of Parliament that has responsibility for oversight on behalf of the legislature of the UK intelligence community.

The Committee sets its own agenda and work programme, with an independent secretariat and investigator. It operates in accordance with a memorandum of understanding reached with Prime Minister. It takes evidence from Government Ministers, the heads of the intelligence Agencies, officials from the intelligence community, and other witnesses as required. The Committee produces an Annual Report on the discharge of its functions. The Committee may also produce Reports on specific investigations. The most recent, Privacy and Security: A modern and transparent legal framework, fed into the reform process reflected in the IPA. The Committee may also prepare confidential reports that it submits only to the Prime Minister.

Under the IPA, an Investigatory Powers Commissioner will keep under review, audit, inspect and investigate the exercise of powers by public authorities, including national security notices. The Commissioner will be supported by Judicial Commissioners, who will review Ministerial warrants, in accordance with judicial review principles, and approve or reject.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Currently, the oversight of the Interception Commissioner and the ISC is ex post. Under the IPA, it is proposed that Judicial Commissioner will grant ex ante approval of all ministerial warrants.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes. In Liberty and others v Secretary of State for Foreign and Commonwealth Affairs and others [2015] UKIPTrib 13 77-H. There were no consequences, as the breach was held to be technical in nature.

11. Do law enforcement authorities need court orders to intercept communications?

In most cases, a warrant to intercept is granted by a Minister on behalf of the Government, not by the courts. However, where the data is being stored in the course of its transmission, then it can be accessible to law enforcement agencies under a court order.

12. How can law enforcement authorities compel companies to provide access to data?

Both Ministerial and Court ordered warrants are enforceable. RIPA warrants are enforceable through civil proceedings, while a failure to

comply with a court order could give rise to contempt of court proceedings. It is also a criminal offence to fail to comply with a warrant under RIPA.

Under s. 11(4) RIPA telecommunications companies are required to assist in the obtaining of communications content.

Under Chapter II Part I of RIPA, providers have a duty to supply communications attributes data.

Similar rules will be applicable under the IPA. However, service providers outside of the UK will have a defence, in certain circumstances, where they are subject to conflicting legal requirements in the jurisdiction in which they are established.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Not before the courts, but may push back on a request if it is considered overbroad. In R (NTL Group Limited) v Ipswich Crown Court [2002] EWHC 1585 (Admin), the provider brought proceedings to clarify that it was able to comply with the court order without acting in breach of criminal law under RIPA.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Article 8 of the European Convention on Human Rights confers upon individuals a right to respect for private and family life, their home and their correspondence. By virtue of the Human Rights Act 1998 (HRA), proceedings can be brought against public authorities, such as law enforcement agencies, for breach of their Article 8 rights.

Article 7 of the EU Charter of Fundamental Rights echoes this, by stating that everyone has the right to respect for their private and family life, their home and communications. No right of action would

exist against a company for disclosing data in compliance with its statutory duties under RIPA.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

In principle, there is nothing restraining the taking of an action against a U.S. company in the UK, provided the relevant jurisdictional thresholds are met. See, for example, Google Inc v Vidall-Hall and others [2015] EWCA Civ 311.

The U.S. Government is however protected from any action by virtue of sovereign immunity, for acts done in a governmental capacity, as opposed to a commercial capacity. This immunity extends to 'emanations of the State', such as the National Security Agency in the U.S."

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

This could constitute a violation of the Data Protection Act 1998, which could enable a data subject to obtain damages. However, under s. 29(3), data controllers are exempt from their non-disclosure obligations when disclosing personal data for law enforcement purposes.

17. Are data subjects notified if law enforcement accesses their data?

No, it is a criminal offence to disclose the existence of, or any conduct relating to an interception warrant or notice for communications attributes data.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

The IPA, when brought into force during the course of 2017, will establish a more consolidated regime for all law enforcement powers to intercept. It will replace RIPA, Part 1. The IPA will grant powers for targeted and bulk interception; targeted and bulk acquisition of communications data; data retention; targeted and bulk equipment interference and the obtaining of bulk personal data sets.

United States

Lothar Determann
Palo Alto
Tel: +1 650 856 5533
lothar.determann@bakermckenzie.com

Brian Hengesbaugh
Chicago
Tel: +1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Michael Mensik
Chicago
Tel: +1 312 861-8941
michael.mensik@bakermckenzie.com

Michael Egan
Washington, D.C.
Tel: +1 202 452 7022
Michael.egan@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

Yes.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

No.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Generally, yes.

4. How can intelligence services compel companies to provide access to data?

Generally through warrants, subpoenas, other court orders.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, U.S. intelligence services cooperate and exchange information with services of Australia, Canada, New Zealand and the UK (Five Eyes Alliance) and others.

6. Are data subjects notified of surveillance by intelligence services?

No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

Yes.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Yes. Congress, and various committees appointed therein, monitor and regulate intelligence programs and authorize and appropriate funds for such programs. In addition, certain surveillance and intelligence activities are also monitored by the Foreign Intelligence Surveillance Court.

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

Generally, ex ante.

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

Yes, historically, there have been publicized cases, including those related to the Snowden disclosures. Courts have enjoined intelligence services from engaging in certain surveillance activities and additional oversight and restrictions have been imposed on such activities by Federal law and Executive Orders. In March 2017, the current U.S. President (Trump) has publicly complained that the previous U.S. President (Obama) had ordered wiretap surveillance on Trump's election campaign and various investigations into the matter are pending.

11. Do law enforcement authorities need court orders to intercept communications?

Generally, yes, to intercept the content of communications or obtain location data by interception methods.

12. How can law enforcement authorities compel companies to provide access to data?

Generally through warrants, subpoenas, other court orders.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

Yes.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

Against the government: 4th & 14th Amendment, Privacy Rights Act of 1974, federal and state electronic communications privacy protections (e.g., wiretap acts), state constitution protections, liability, and damages, among others.

Against companies: electronic communications privacy protections, contractual rights, injunctions, damages, attorneys fees.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

Yes, most U.S. privacy laws protect individuals without regard to citizenship and courts will generally take jurisdiction against U.S. companies regardless where plaintiff is located. The 4th Amendment protections are limited to searches on U.S. territory, but the California Constitution and most statutes, torts and other privacy laws are not so limited. The U.S. Federal government enjoys some immunities and privileges against court proceedings, but under 42 U.S.C. Section 1983, individuals are protected against civil rights abuses including unconstitutional privacy intrusions. There may also be available remedies against U.S. companies such as electronic communications privacy protections, contractual rights, injunctions, damages, attorneys

fees, as well as potential protections available under the EU-U.S. and/or Swiss/U.S. Privacy Shield Programs, if applicable. In 2016, the U.S. government has extended privacy protections under the U.S. Federal Privacy Act to residents of numerous allied countries, including all EU member states, according to the Judicial Redress Act of 2015.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes.

17. Are data subjects notified if law enforcement accesses their data?\

Yes, in many cases.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

Following the Snowden revelations in 2013, the US have taken various steps to reign in government surveillance and afford more privacy protections to residents and foreigners.

Vietnam

Yee Chung Seck
Ho Chi Minh City
Tel: +84 8 829 6234
yeechung.seck@bakermckenzie.com

Chi Anh Tran
Ho Chi Minh City
Tel: +84 8 3520 2625
ChiAnh.Tran@bakermckenzie.com

1. Do intelligence services operate surveillance programs to protect national security?

The State bodies have broad authority to conduct surveillance programs to protect national security.

2. Are intelligence services authorized to conduct surveillance for an economic purpose?

State bodies are authorized to conduct surveillance programs to protect national security. (which may include economic intelligence in the national interest) Industrial espionage (i.e. private surveillance) is generally not allowed in Vietnam.

3. Do intelligence services need court orders to intercept calls, emails or other communications?

Generally, no.

4. How can intelligence services compel companies to provide access to data?

By law, companies must provide, inter alia, access to data upon the relevant authority's request. A court order is generally not required.

5. Are national intelligence services cooperating and exchanging information with foreign services?

Yes, to a certain extent, intelligence may be exchanged between Vietnam and certain other countries. However, the details of such exchange arrangements are generally not made public.

6. Are data subjects notified of surveillance by intelligence services?

Generally No.

7. Do data subjects have a right to court review of surveillance measures taken by intelligence services?

By law the data subjects may sue the relevant authority before a court. However, in practice we are not aware of any cases where a data subject has exercised such a right.

8. Are other governmental bodies (Ministry, Parliamentary Committee etc.) notified of (individual) surveillance measures taken by intelligence services?

Generally, no. Only the bodies engaging in the surveillance measures are made known (e.g. the Ministry of Defense, Ministry of National Security).

9. If yes, are the governmental bodies (Question 8) notified ex ante or ex post? Do they have a right to object to the measures?

10. Are there publicized cases that national intelligence services have violated applicable laws relating to surveillance measures? What were the consequences? Name examples.

No.

11. Do law enforcement authorities need court orders to intercept communications?

Generally No.

12. How can law enforcement authorities compel companies to provide access to data?

By law, companies must provide, amongst others, access to data upon the relevant authority's request in connection with administrative, criminal or civil action.

13. Can and do companies challenge orders to provide personal data to law enforcement authorities? Provide examples.

By law companies may sue the relevant authority before a court. However, in practice we are not aware of any cases where a company has successfully exercises this right.

14. What privacy rights do individuals have against government agencies and companies if companies share personal data with government?

By law, companies are required to share personal data with government upon the government's request in connection with administrative, criminal or civil enforcement investigations or activities.

15. Can European data subjects assert privacy rights against U.S. companies and the U.S. government (and vice versa under European laws)?

By law, yes. However, in practice we are not aware of any cases where European data subjects have asserted their privacy rights against companies or the Vietnamese government.

16. Are companies liable to data subjects if they disclose data to the government without sufficient legal bases? Provide examples.

Yes, companies may be liable to pay compensation based on a civil action brought by a Data Subject, and administrative sanctions

(monetary fines) may also apply. Although unlikely, the relevant personnel of the company may also be criminally prosecuted.

However, in practice we are not aware of any cases where a company discloses data to the government without sufficient legal basis.

17. Are data subjects notified if law enforcement accesses their data?

By law, generally No.

18. Are there any other key points to note about surveillance in this jurisdiction, whether by intelligence services or law enforcement?

No.