Morrison & Foerster Client Alert

March 10, 2015

Who's Winning in the Battle Between Privacy and Security?

The State of Surveillance Law in Europe

By Susan McLean, Sotirios Petrovas and Mercedes Samavi

In recent years, there has been an ongoing struggle between privacy and security, with many governments looking to increase their surveillance powers in the name of fighting terrorism and protecting the population. Following the Snowden revelations, it seemed that the dial had begun to turn toward privacy. However, recent events – in particular, the Charlie Hebdo attack in Paris in January 2015 and the Sony hacking in December 2014 – appear to be pushing governments and public opinion back towards improved security, at the expense of personal privacy. In this Alert, we consider the current state of surveillance laws in Europe.

BACKGROUND

In 2014, the tide of opinion appeared to be turning in favor of privacy. Firstly, in a landmark ruling in spring 2014, the European Court of Justice (the **ECJ**) invalidated Directive 2006/24/EC (commonly referred to as the **Data Retention Directive**), on the grounds that "*it interfere[d] in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.*" The Data Retention Directive had long been criticized by privacy campaigners; however, its invalidation arguably created more problems than it solved, with EU Member States consequently taking conflicting positions on data retention in the wake of the ECJ's judgment and recent international and political events.

Later in 2014, the Article 29 Working Party[1] issued its "Working Document on surveillance of electronic communications for intelligence and national security purposes". The Working Party commented that "*massive, structural, indiscriminate, secretive, repetitive or unlimited data transfers*" are illegal and unjustifiable under existing data transfer mechanisms, such as Safe Harbor.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346
Lokke Moerel 44 20 79204054
Alex van der Wolk 44 20 79204054

Brussels
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Amy Collins 44 20 79204180
Susan McLean 44 20 79204045

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

[1] The group made up of the data protection authorities of each EU Member State, the European Data Protection Supervisor, and the European Commission.

In 2014, the United Nations also made its stance on the struggle clear;[2] it stated that mass surveillance poses a direct challenge to international law, is not proportionate, and is "*indiscriminately corrosive of online privacy*". This has been echoed by various major privacy groups, as well as high-ranking officials such as the UK's surveillance commissioner, Tony Porter, who stated in early January 2015 that an increased use of surveillance technology risks altering the "*psyche of the community.*[3]"

However, the recent extremist attacks have reignited the debate about surveillance powers. The European institutions are currently examining further actions on countering terrorism, and the European Commission (the **Commission**) has promised to release a new agenda on security in the coming months for the years 2015-2020. So the future is uncertain but, for now, what is the state of surveillance law in Europe?

THE DATA RETENTION DIRECTIVE

Background and Rationale

The Data Retention Directive was adopted in February 2006, in the aftermath of the terrorist attacks in New York in 2001, Madrid in 2004, and London in 2005. Its aim was to enable law enforcement agencies to gather communications data efficiently in the on-going fight against "serious crimes", a broad term that the Data Retention Directive purposely omitted to define, but was generally understood to cover organized crime and terrorism.

The Data Retention Directive required Member States to adopt laws that oblige electronic communications service providers to retain, for a minimum of six months and a maximum of 24 months, all traffic and location data that they generate in the course of providing their services. The types of data covered included data that make it possible to track and identify the source, destination, and frequency of every communication, including communications that are "unsuccessful," but excluding the actual content of those communications. The Data Retention Directive required that any data retention activity should only be used for: (i) investigation; (ii) detection; and (iii) prosecution of serious crime. Any data collected could be shared with the competent authorities pursuing such purposes in accordance with strict legally defined procedures.

Controversies and Criticism

The Data Retention Directive was fiercely criticized by campaigners concerned over the potential infringement of privacy rights and the lack of guidance on implementation, which led to a mosaic of heterogeneous national laws. It also faced numerous legal challenges at both an EU and a national level, from courts in Bulgaria, Romania, Germany, Hungary, Cyprus, and the Czech Republic, concerned that the Data Retention Directive conflicted with constitutional rights.

THE ECJ RULING

On 8 April 2014, following requests for a preliminary ruling from the Irish High Court and the Austrian Constitutional Court,[4] the ECJ ruled that the Data Retention Directive was invalid retroactively from its inception, because the blanket collection of communication records amounted to "serious interference" with the fundamental rights to private life and protection of personal data (the **Ruling**). The ECJ stated that the Data Retention Directive's scope, retention period, and

[2] Promotion and Protection of Human Rights and Fundamental Freedoms When Combatting Terrorism.

[3] http://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent.

[4] Joined cases C-293/12 and C-594/12.

security justifications were ill-defined, and concluded that, in order to be lawful, the data retained should be limited to a specific purpose and length of time that is determined objectively. Despite the Advocate General's opinion that the effects of invalidity should be suspended until the adoption of a new data protection regulation, the Ruling rendered the Data Retention Directive void, with immediate effect.

By rolling back the legal foundation for national data retention laws and regulation across the EU, the Ruling has created a legal vacuum and a political headache for Member States and their governments. Although, from a legal standpoint, national laws remain unaffected by the annulment of the Data Retention Directive (Member States, in principle, have the sovereign right to enact legislation in the absence of, or in contradiction to, an EU directive), such national laws run the risk of violating the European Convention of Human Rights, on the grounds of being unconstitutional.

THE EU RESPONSE

To date, the response to the Ruling at the EU level has been generally consistent.

In April 2014, the European Data Protection Supervisor welcomed the Ruling and stated that it anticipated that the Commission would consider the need for a new directive to be enacted to "*prevent Member States from keeping or imposing the same legal obligations nationally as laid out in the now invalid [Data Retention Directive].*"[5] It also stated that the judgment meant that the EU should "*take a firm position in discussions with third countries, particularly the U.S.A. on the access and use of communications data of EU residents.*"

In August 2014, the Working Party[6] adopted a statement[7] welcoming the Ruling and urging Member States and competent European institutions to evaluate the consequences of the Ruling on national data retention laws and practices in the EU. The Working Party also provided recommendations on the actions that Member States should take in response to the Ruling. These included ensuring that there is no bulk retention of data and restricting government access and use to what is strictly necessary in terms of categories of data and persons, subject to substantive and procedural conditions. The Working Party also stated that there must be effective protection against unlawful access and abuse, including the requirement that the storage of data be made subject to the control of an independent authority, ensuring compliance with data protection law. In addition, because the Ruling did not directly affect the validity of national data retention laws, the Working Party has asked the Commission to provide "without further delay" guidance on the consequences of the Ruling, at both a European and Member State level.

In November 2014, the issue was raised again when a majority of the European Parliament's Civil Liberties, Justice and Home Affairs committee (LIBE) stated that the Ruling needed to be reviewed before the EU could agree to a new EU Passenger Name Record (PNR) Directive.[8] On February 24, 2015, LIBE reignited the debate by releasing a Working Document calling for follow-up work on the Parliament's resolution of March 12, 2014. Adopted in the wake of the Snowden revelations, the resolution urged Member States to disclose their mass surveillance activities and laid the foundation for the creation of a "European digital habeas corpus." The follow-up resolution is expected to be published in May 2015.

[5] Press Statement: The CJEU rules that Data Retention Directive is invalid.
[6] https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29.
[7] Statement on the ruling of the CJEU which invalidates the Data Retention Directive.
[8] MEPs debate plans to use EU Passenger Name Record (PNR) data to fight terrorism.

MEMBER STATES' RESPONSES

In contrast, to date, individual Member States' responses to the Ruling have been varied and inconsistent.

UK going it alone?

In response to the Ruling, in July 2014, the UK government introduced the Data Retention and Investigatory Powers Act (**DRIPA**). The Act received fierce criticism from privacy and civil liberties campaigners, with many pointing out that it did not meet the required criteria identified by the Ruling. Indeed, even the Impact Assessment published alongside the draft bill acknowledged the "*risk of being perceived as ignoring the ECJ judgment*".

Key changes under DRIPA include the following:

- the UK government is granted considerable powers to order public telecommunications operators to retain communications data for up to 12 months;
- the Regulation of Investigatory Powers Act 2000 (**RIPA**) is amended so that the UK government can now issue warrants to obtain data from operators that are based outside of the UK; and
- DRIPA broadens RIPA's definition of a telecommunications system so that many web-based telecommunications systems (such as web-based email) are now caught.

Faced with pressure, the UK government conceded that DRIPA would contain a "sunset clause" which means that the legislation will expire on 31 December 2016 and will need to be reviewed in advance of that date. In addition, the UK government accepted a proposal for reports to be provided to the UK parliament every six months on how the new law is working.

Further moves have also been made by the UK to bolster its surveillance powers with a new Counter-Terrorism and Security Bill being introduced to the UK parliament in November 2014. The bill would require Internet Service Providers (**ISPs**) to retain IP addresses in order to identify individual users of Internet services. Campaigners have argued that the new law is an attempt to revive the controversial Communications Data Bill, dubbed the "snooper's charter", which was recently resurrected by peers in the House of Lords in the wake of the Paris attacks, before being dropped in February 2015.

The UK government faced another blow when the UK Investigatory Powers Tribunal (**IPT**)[9] declared on 6 February 2015 that GCHQ's access to emails and phone records and the subsequent interception of such communications by the U.S. National Security Agency contravened Article 8 (right to private and family life) and 10 (right to freedom of expression) of the European Convention on Human Rights. Notably, this judgment is the first time that the Tribunal has ever upheld a complaint relating to one of the UK's intelligence agencies.

And scrutiny of intelligence practices in the UK continues as the government admitted on 18 February, in advance of another hearing before the IPT, that it has been unlawfully monitoring legally privileged communications for the last five years.

[9] The Investigatory Powers Tribunal is an independent public body which investigates complaints about the alleged conduct of public bodies in relation to members of the public under the Regulation of Investigatory Powers Act (RIPA) 2000. This includes complaints about the use of intrusive powers by the UK intelligence services.

When courts decide instead of legislators: The example set by Austria

In sharp contrast to the UK approach, the Austrian Constitutional Court repealed key data retention provisions[10] in June 2014, thereby making Austria the first Member State to effectively bring its domestic law into line with the Ruling. The Austrian decision had immediate effect and constitutes a prompt and loyal implementation of the Ruling into Austrian law; the judgment noticeably contains a near-identical reasoning to that stated in the Ruling, citing overbroad scope, lack of safeguards, and strong interference with privacy rights.

Elsewhere in Europe

- **Germany**, which at one point faced potential sanctions for failing to transpose the Data Retention Directive, was waiting for the ECJ's judgment, before making a decision whether to implement a data retention law. Since the Ruling, Germany has indefinitely postponed its plans and its Federal Data Protection Commissioner Andrea Vosshoff states that Germany should wait "*until EU lawmakers decide*" to enact a new directive.

- Similarly, in **France**, the legislative branch and the French Data Protection Authority (the **CNIL**) have not taken a position on the potential impact of the Ruling on French law. In 2011, the CNIL criticized domestic law implementing the Data Retention Directive, stating it overlapped with other anti-terrorism laws and created legal uncertainty for privacy protection. Prior to this, the Conseil d'Etat held that the interference of data retention with private life was not sufficiently disproportionate, when implementing the domestic law. Generally, commentators observe that France's data retention provisions[11] are likely to remain unaffected by the Ruling, namely as they predate the Data Retention Directive coming into effect. Moreover, France has recently proposed tougher measures than those under the Data Retention Directive, in reaction to the Charlie Hebdo attack; such measures purportedly promise a general mobilization against terrorism, greater responsibility for Internet services, and increased cooperation with technology companies.

- In **Spain**, a new data retention law was introduced into pre-existing legislation relating to electronic communications and public networks in May 2014.[12] As such, Spanish law was brought in line with the Ruling; for example, the amended law now provides that information accessed by security agencies is limited to such information that is "*essential to the achievement of the purposes*" of the law.

- In July 2014, the Constitutional Court in **Romania** declared its data retention law to be unconstitutional. The Constitutional Court decided that access to retained data by law enforcement can only take place after judicial consent has been provided, and such access must meet a proportionality test closely resembling that which was stated in the Ruling. Romanian ISPs are not obliged to delete retained data; instead, they must refrain from collecting such data going forward, pending adoption of new data retention legislation that meets the Constitutional Court's test.

- In **Sweden**, where the Data Retention Directive was never keenly supported by citizens and businesses, Swedish

[10] The decision (BGBl I 44/2014) repealed provisions in the Telecommunications Act 2003, the 1975 Code of Criminal Procedure, and the Security Police Act.

[11] Most notably, Article L34-1 of the Code for Postal Services and Electronic Communications.

[12] Law 9/2014 on Telecommunications introduced new provisions into Law 25/2007.

ISPs deleted all retained data promptly after the Ruling. Although at the time of the Ruling, the Swedish Post and Telecom Authority (the **PTS**) did not demonstrate an intention to go against the Ruling, in August 2014, following a government decision to uphold the Data Retention Directive, the PTS threatened to impose fines on ISPs if they did not comply and save customer communications data for six months. After reviewing a complaint from Swedish Internet carrier Bahnof, the Commission has now agreed to investigate PTS's actions.

- **Denmark** was one of the only countries where its government conducted a legal analysis on whether its existing legislation on the data retention would meet the ECJ's proportionality test. The report was issued in June 2014, and it found that Danish law is in line with the Ruling.[13] This decision may well find renewed support in the wake of the Copenhagen attacks in February 2015.

- In **the Netherlands**, in November 2014, the Dutch government indicated that the Dutch data retention legislation will remain in place despite the Ruling. However, the procedures for accessing retained data will be tightened, in particular, data stored for the full 12-month period will only be accessible in the context of investigating serious crimes which carry a sentence of eight years or more. Access will also require approval from a magistrate. This approach has resulted in pushback from the country's criminal lawyers' association, which has joined forces with the Dutch Association of Journalists, as well as other civil rights organizations to launch a legal challenge against the government; the District Court of the Hague will hear the challenge on 18 February 2015. The Dutch Data Protection Authority has also opposed the legislation.

CONCLUSION

While the Ruling has been considered a step forward for citizens' privacy rights across Europe, arguably the decision has not yet had the intended effect. Instead of encouraging EU institutions and Member States to converge on a new EU legal regime for data retention, the ECJ has created a lacuna in its law, opening the door to a cacophony of assorted interpretations of what the Ruling means for domestic legislation. It's clear that a definitive response to the Ruling is needed. The EU is not oblivious to this; a report by the Council of Europe's Parliamentary Assembly in January 2015 stated that "*a legal framework must be put in place at the national and international level which ensures the protection of human rights, especially that which secures the right to privacy.*"[14]

Jumping across the Atlantic Ocean, the U.S., despite the National Security Agency revelations in 2013, is apparently not ready to follow suit and rein in its data retention legislation. In November 2014, the U.S. Senate blocked a drastic overhaul of the NSA program that collected records of Americans' phone calls in bulk, thus defeating the intentions of an alliance of technology companies including Google and Microsoft. More recently, President Obama has been pushing private companies to share sensitive information on cyber threats with the government, in order to ward off any potential attacks.

However, with pressure from international organizations such as the UN, technology companies, privacy campaigners, and individuals, this issue is certain not to go away anytime soon, either in Europe or the U.S. Indeed, studies show that individuals are increasingly concerned about how companies and governments use their personal data.[15] This means that many companies are starting to change their perspective on privacy. Increasingly, companies are beginning to

[13] Report by the Ministry of Justice (in Danish only).
[14] Committee on Legal Affairs and Human Rights – Mass surveillance report.
[15] For example, Pew Research Centre Study – Public Perceptions of Privacy and Security in the Post-Snowden Era.

appreciate that privacy is no longer just a question of compliance; demonstrating that you take privacy seriously can be used as a differentiator and make good business sense. Accordingly, U.S. technology companies that process significant volumes of customer data in Europe are understandably concerned by the impact of developments, such as the Snowden revelations, on their European business. Various companies such as Amazon have responded by opening local data centers in Europe[16] and we envisage that this trend for local storage for privacy reasons is likely to increase.

In terms of data retention laws specifically, service providers, which are subject to the applicable data retention legislation in each Member State, will need to pay close attention to any changes in such legislation and the official position of data protection authorities with regard to the enforcement of such rules. Unfortunately, at least for now, multinational providers will not be able to apply a consistent data retention policy across their business, but will need to ensure that they meet all local data retention requirements.

We expect that over the next year the Commission's attention may be primarily focused on ensuring the Data Protection Regulation is passed. However, in light of recent terrorist attacks, we expect that the Commission is also going to have to return to the question of how surveillance and data retention powers can be proportionately balanced with principles of privacy. And conversations between governments, campaigners, and the general public across Europe will continue in terms of where the line between personal liberty and protection should be drawn. Finally, the adoption of the Regulation may well be impacted by the fight over government access to, and use of, personal information. After all, the contrast in the ways the Data Retention Directive itself was received across Member States is telling of a more profound lack of consensus — if not actual discord — on core privacy issues in Europe, which may in part explain why the Regulation is taking so long to be adopted.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.

[16] http://www.theregister.co.uk/2014/10/23/aws_frankfurt_region/.