OPINION OF GEOFFREY ROBERTSON QC

1. I am asked to advise Facebook about the consequences of the European Court of Justice decision in *Schrems v Data Protection Commissioner*[1], which struck down the "safe harbour" regime under which the Commission permitted European data collectors to transfer data to servers in the USA without infringing the European regulations which mandate an 'adequate' level of privacy protection for third country transfers. This ruling entirely accepted "facts" stated by the Irish High Court, which had not examined US law but had endorsed the revelation by Edward Snowden that PRISM and other programmes had enabled the NSA to engage in bulk or "generalised" collection of such data without being bound by any laws or rules relating to data processing. The European Court of Justice (ECJ) ruled that data transfers to a third country were prohibited under European law unless that country's domestic law "ensured an adequate level of protection", which is "essentially equivalent" to what it assumed to be a "high level of protection" guaranteed within the European Union by the *Charter of Fundamental Rights*. The ruling begs the question – which neither the Court nor its Advocate General addressed – of what "adequacy" means in terms of the actual protections, "essentially equivalent" to those in European law, which must be provided by US law before European data can ride safely at anchor on a server located in America.

2. In this opinion, I shall begin with an analysis of *Schrems*, noting its limitations and the Court's apparent misunderstanding of established US

[1] Case C-362/14, 6 October 2015

law and its failure to take any account of the considerable changes in US law consequent upon the Snowden revelations. I consider the impossibility of applying the notion of "essential equivalence" to the actual privacy protections offered in European states where the interference with privacy is justified on 'national security' grounds as these are so diverse and often conflicting and are themselves, in many cases concerning 'national security' surveillance, incapable of delivering on the guarantees of the Charter. A more satisfactory approach is to extrapolate the principles relating to secure surveillance that are being developed by the European Court of Human Rights, pursuant to Article 8 of the European Convention, (Article 8 being the privacy protection article equivalent to that in the Charter) and to consider how they match US law principles that were developed long before Snowden, and have been extended in consequence of his revelations.

3. This comparison will reveal that US law is, in fact, more robust in relation to controls over government surveillance (in terms of constitutional foundation, Congressional oversight and checks by judicial and independent experts) than that which exists in many – arguably all - European states. European protections appear to be diminishing, rather than increasing, as national security concerns following the Paris massacres have encouraged member states to allow, with few controls, the bulk collection of data by intelligence services. Applying the *Schrems* test today would show that American citizens have greater privacy safeguards, post-Snowden, than residents of Europe although the further and vital question is whether and to what extent those safeguards now extend to European citizens as well as Americans in

respect of data held upon them in America. On this question the issue – of whether such data can be transferred to the US – really turns, and the answer must involve analysis of the foundations of US privacy law and of the post-Snowden reforms, in particular the implementation of a Presidential Policy Directive (issued by President Obama on 17 January 2014) requiring similar (and in any view, "adequate") treatment for foreigners ("Non-US persons" in the argot of US law and administration).

The *Schrems* Decision

4. Schrems is an Austrian privacy activist who complained to the Data Protection Commissioner in Ireland (Facebook's European base) that the company was transferring data to its US servers in breach of Directive 95/46 which prohibits such transfers to a "third country which does not ensure an adequate level of protection". The Commissioner refused to investigate his complaint, on the ground that she was bound by Decision 2000/520, by which the European Commission decided that the "safe harbour" agreement with the US meant that this country was conclusively presumed adequately to protect transferred personal data. Schrems appealed against the Commissioner's refusal to entertain his complaint, and the High Court referred the issue to the European Court of Justice.

5. The *ratio* of the ECJ ruling was narrow – its actual decision was that the Commissioner was not bound to reject the complaint by application of Decision 2000/520, and must proceed to examine it. However, in the process of reaching that decision, the Court determined not only that Data Commissioners had an independent duty to examine complaints

irrespective of earlier Commission decisions, but that the Commission itself had a duty to check periodically whether its previous findings on third country adequacy were still "factually and legally justified", especially when evidence came to light that they were not.[2] Such evidence had been accepted by the Commission itself in 2013: it had noted Snowden's revelations about the PRISM programme, which it believed had allowed European data transferred to the US, including data transferred under "safe harbour", to be accessed and processed "beyond what is strictly necessary and proportionate to the protection of national security", without safeguards available to US citizens and without any prospect of judicial redress[3].

6. This led the Court to the portentous conclusion that the Commission's earlier decision, 2000/520, endorsing "safe harbour", was invalid because "protection of the fundamental right to respect for private life at EU level" requires exceptions to that right to be limited by the principle of strict necessity[4]. The court (as will appear, mistakenly) assumed that US law permitted the hoovering up data "on a generalised basis"[5]; access to it by spying agencies "on a generalised basis"[6] and lacked any legislative basis to enable a person wrongfully targeted to have an effective judicial remedy[7]. These assumed features meant that US law was inadequate by European standards. Ironically, having required the Commission to ensure that its decisions were up-to-date and "factually and legally accurate", the Court did not itself apply – or

[2] Ibid, para76
[3] See para 90, and its references to earlier paras 22,23 & 25
[4] 92
[5] 93
[6] 94
[7] Para 95

refer to – either the protection for privacy long mandated by the Fourth Amendment or to changes in American law and practice after – and partly as a result of – the Snowden revelations. As will appear, its beliefs that the PRISM programme was one of 'bulk' or generalised collection of data, and that non-nationals have no rights to remedy under US law, are incorrect. Application of the "essential equivalence" test requires that the American law and practice which is to be placed in the balance against its European counterpart is that which applies to personal data today and is correctly understood by the Commissioner or court called upon to apply the test.

7. The Court held that the Commission's 'safe harbour' decision was invalid, and that 'safe harbour' itself does not satisfy the Charter Principle 7 (the right to privacy), 8 (the right to have personal data properly processed) and 47 (the right to an effective remedy). It was less clear – in fact, it was opaque – as to how any 'safe harbour II', or other mechanism for appropriate transfer of personal data from Europe to the US, might work, or how US law and practice was to be compared with European law (and domestic law in European states) to ascertain "essential equivalence". It must be remembered that neither Facebook nor the US government were represented, either in the High Court or in the European Court of Justice. There was no evidence about American law, and despite the asserted duty on the Commission to keep its decisions up-to-date, there was little effort to understand US law and no comprehension on the part of the Court or its Advocate-General of the changes that Snowden's 2013 revelations had brought about in US domestic law and practice in 2014 and 2015.

8. 'Safe Harbour' was, in effect, a code of conduct to which 3,200 organisations subscribed[8]. It was struck down on the basis of an unexamined allegation by Edward Snowden that NSA had established PRISM in 2009 to obtain unrestricted access " on a casual and generalised basis" to mass data stored on US servers.[9] (This is not factually correct, although it reflects many media misinterpretations of PRISM). However, there was no discussion by the Court of the overriding "national security" exemption for collection of data in breach of privacy principles, which applies in both US and European law and which must be the focus of the "essential equivalence" test.

9. It is important to emphasise that the European Union and its instrumentalities have no power to give directions on national security, a matter that is reserved to its member States (See Article 4(2) of the EU Treaty and Article 3(20) of the Data Protection Directive). The national security "exemption" will however be a matter to be considered by the Data Protection Commissioner in Ireland, as part of her investigation into whether Facebook users "have significant guarantees (in the US) enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data"[10] by organisations concerned with US (and, to an extent, international) security – especially the NSA, CIA and FBI.

[8] See Advocate General's Opinion, 23 September 2015, para 13
[9] Ibid, para 26, 35-6, 123
[10] Judgement, para 91

10. The Court decreed that the Commissioner's task is to decide whether the United States "in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights *essentially equivalent* to that guaranteed in the EU legal order"[11]. This is the only elucidation it offers of Article 25 Directive 95/46, which requires third countries "to ensure an adequate level of protection... assessed in the light of all the circumstances surrounding the transfer operation..." These circumstances include the nature of the "third country" – i.e. the USA, a NATO ally whose intelligence is shared with European nations in respect of the war against terrorism and against the development of weapons of mass destruction.

11. The word "adequate", in the English language, can mean that which is merely sufficient or satisfactory, although as the Advocate-General notes in his opinion, this is of lesser semantic scope than the French meaning of "*adequat*", which is "appropriate". The latter meaning begs the question "appropriate to what?" which the Advocate-General answers by reference to "attaining a high level of protection of fundamental rights". But this is merely an aspiration, set out in item 10 of the Preamble to Directive 95/46 - national laws must "seek to ensure a high level of protection in the Community". A privacy law may be "adequate" without guaranteeing "high level" protection. It seems to me that the 'appropriate' level of protection in the third country is that which satisfactorily – or sufficiently – reflects (or is effectively equivalent to) the legal protections actually afforded to personal data sought for national security purposes in the European Union. Articles 7, 8 and 47 of

[11] Para 96

the Charter, as explicated by Articles 8 and 13 of the European Convention of Human Rights, set out European privacy principles, which are not dissimilar to the principles endorsed by US law. But the question is not resolved by comparing verbiage – there must be an examination not only of the laws, but of what these laws mean in practice, in a national security context. There must be some assessment of the constitutional roots and the history of this particular liberty in America and in Europe, its strength in popular support and its vulnerability to shrinkage when balanced against the need to deal with international terrorism.

The Foundation of Privacy Protection.

12. The dimension entirely lacking in the Court's comparison between Europe and the US, but which is in my judgement relevant as a first step in any consideration of the "adequacy" of US protection, is the basis upon which that protection rests. There was no legal protection of privacy in England until the 1760s, when America was still an English colony. That was when cases concerning the government's "general warrants" to raid the home and printing presses of John Wilkes and his associates were decided. *Entick v Carrington* [12] and *Wilkes v Lord Halifax*[13] determined that no state official may enter a citizen's home or business without the authority of a legal warrant, and that no warrant was lawful if it failed to specify the kind of material which was sought. "General Warrants" were illegal. These cases – ignored by British forces in the American colonies – inspired, after the War of Independence, the

[12] 19 State Trials 1029
[13] [1763] 19 State Trials 981

great principle in the Fourth Amendment to the Bill of Rights 1791, namely

> *"The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probably cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".*

13. This can be regarded as the first modern privacy law, and its elaboration, in a seminal *Harvard Law Review* article by Brandeis & Warren in 1896, inspired modern legal thinking in Europe and elsewhere, about the need to protect privacy and how law might achieve that goal. In 1934, the *US Federal Communications Act* provided that wiretap evidence must not be disclosed and in 1967 the Supreme Court ruled, in *Katz v US*, that the Fourth Amendment required that in general, all secret surveillance by state agents be authorised by a warrant granted by a judge: citizens had a "reasonable expectation of privacy" which would be upheld by the courts.[14] The Church Committee, in 1975, exposed unauthorised electronic surveillance, and in 1978 the *Foreign Intelligence Surveillance Act* (FISA) established a court to hear (albeit in secret) requests for orders to obtain foreign intelligence[15]. The judges of that court are selected by the Chief Justice, and are independent of government.

14. Even at this late stage, European countries had few, if any, laws regulating secret surveillance, and the ECHR had not begun its task

[14] With certain exceptions, such as where reasonable surveillance is necessary in exigent circumstances or for "special needs".
[15] Foreign Intelligence Surveillance Act 1978, 4 50 USC-180, et seq

(which started with the cases of *Klass* and *Malone* decades after the Convention entered into force), of identifying what safeguards Articles 8 (the right to privacy) and 13 (the right to an effective remedy) required. Meanwhile, it had been Eleanor Roosevelt's UN Committee which (in a draft recommended by the American Bar Association) inserted privacy protection into the *Universal Declaration of Human Rights* ("No-one shall be subjected to arbitrary interference with his privacy, family home or correspondence...").

15. This reflected the Fourth Amendment, and was in its turn copied in Article 8(i) of the 1951 ***European Convention on Human Rights***.

> 8(1) *Everyone has the right to respect for his private and family life, his home and correspondence.*
>
> 8(2) *There shall be no interference by public authority with the exercise of this right except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights or freedoms of others".*

16. This is now the basis for the alleged 'high level' of European protection, through the judgements of the European Court of Human Rights (ECHR) elucidating, by decisions on Article 8 of the Convention, rights that are now entrenched in EU law by Articles 7, 8 and 47 of the Charter. It may be noted that in terms, Article 8 is not 'high level' at all – the exemptions

in 8(2) are very wide, and the interests of national security and public safety would excuse even bulk downloading if that could be shown possibly to prevent a terrorist atrocity. For the purposes, however, of an 'adequacy' comparison, I simply note that privacy protection has, historically, a much firmer footing in the US than anywhere else and that European privacy protections have themselves been influenced by US jurisprudence. With the exception perhaps of Sweden, European states evinced little interest until the late twentieth century in combating invasions of privacy. The UK, for example, had completely ignored the subject: privacy was not protected by statute or common law, and telephone tapping was conducted entirely at the discretion of the state until *Malone* forced legislation in 1985. In comparing constitutional foundations, legal history and commitment to privacy as a fundamental liberty, US traditions are "high level" whilst those in Europe are barely adequate.

European Safeguards.

17. Beginning with *Klass v Germany*[16] in 1978 and *Malone v UK*[17] in 1985, and more recently *Weber & Saravia v Germany*[18] and *Szabo & Vissy v Hungary*,[19] the European Court of Human Rights has been developing the safeguards required for the forty-seven Council of Europe states (which of course include the twenty-eight EU states) to live up to the guarantee in Article 8. It must be understood that these safeguards have been devised mainly in respect of telephone tapping and other forms of *targeted* surveillance rather than bulk data collections used to winnow out possible

[16] [1978) 2 EHRR 214
[17] [1985] 7 EHRR 14
[18] Application no 54930/00, 26 June 2006
[19] [2015] ECHR 883

terrorist-related information, e.g. by examining posts with "key words". Most cases concern law enforcement by police out to discover serious crime, as distinct from intelligence services monitoring potential terrorist activity or other threats to national security. The law in respect to safeguards in cases of suspected terrorism is permissive in relation to interception, especially following the Paris atrocities and the general acceptance of the need to monitor potential jihadis – a surveillance of persons and organisations that may need to continue for some years. However, the main ECHR cases do suggest that a number of safeguards are required by Article 8:[20]

I. Established Law.

Secret surveillance must be "in accordance with law" – i.e. there must be legislation, or else some binding regulation (underpinned by rules that are sufficiently accessible) authorising secret interception and processing of data.

II. Specificity

There must be a clear definition of the conduct, or suspected conduct, in relation to which the power of surveillance may be deployed and the test – e.g. "reasonable suspicion" - for that deployment.

III. Independent Authorisation.

Interception warrants should be judicially authorised, by a judge or a Court or a Tribunal, or else by an independent body, which can expertly

[20] These requirements have been variously stated and organised under various headings in the case-law: in relation to telephone tapping, see for example the six safeguards listed in para 95 of *Weber and Saravia*, above.

assess whether there is a security justification for the intercept. It seems, however, that authorisation by a government Minister (as in the UK) is acceptable, although the decision in *Szabo & Vissy* questioned whether ministerial approval was sufficient, at least in the absence of other safeguards.

IV. Clarity of Process.

There should be a system for ensuring that the warrant, when granted, does not permit over-broad surveillance, i.e. that collateral intercepts of data about persons not under suspicion are destroyed, and that there is an approved procedure for examining and storing the data.

V. Data Protection.

There should be satisfactory rules, reflecting data protection standards, for communicating the data e.g. to police or other law enforcement bodies.

VI. Time frame and Destruction of Stored Data.

There should be a period (extendable, but by authorisation) for the surveillance operation, and a definite time at the end of which stored data must be destroyed.

VII. Oversight.

This should take the form of annual reports to Parliament or to a data authority, and preferably some general oversight of the surveillance system by an independent body.

VIII. Redress.

There must be an opportunity to complain, and to obtain and effective remedy through a judicial process. (See Article 13 of the ECHR)

18. The approach of the European court in the first case of 2016 to consider national security surveillance, namely *Szabo & Vissy*, was not to insist on the presence of all eight safeguards. It looked at the position in the round and recognized that the consequence of international terrorism has been a "*massive monitoring of communications"*. However, this cannot be conducted by an unfettered executive power – there must be safeguards that attempt to confine it of cases of "*strict necessity*" for the obtaining of vital intelligence. In this respect, the court said that the most important safeguard will be some form of independent judicial oversight. It had no difficulty in finding that a special anti-terrorist surveillance law breached Article 8 because "*it was possible for virtually any person in Hungary to be subject to secret surveillance*." There was no need for a warrant or for production of any information to any authorising body, and there was no clear procedure for ending the surveillance and no possibility of a remedy. The only oversight was an annual report which did not mention individual cases and was delivered in secret to a parliamentary committee. The case, which was not a Grand Chamber decision, provides an example of national security surveillance which breaches European law because it provided no safeguards at all. It does not answer the question of what safeguards are necessary for national security surveillance in European law.

19. There is some suggestion in *Schrems* that European law prohibits bulk collection of data *per se* – see para 94. I do not consider that this is correct: bulk collection is acceptable, in a national security context, if (but only if) it is subject to safeguards that ensure it remains "strictly necessary and proportionate to the protection of national security". This is certainly the view of the UK's Independent Reviewer of Terrorism Legislation, David Anderson QC, whose recent Report recommends a "bulk communications data warrant"[21]. In *Weber and Saravia*, the Court upheld a German law which permitted "strategic monitoring" on anyone's telephone (as distinct from "specific monitoring of targeted telephone numbers") and emphasised that the European Court of Human Rights has "*consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security*"[22].

20. This is important: the "margin of appreciation" doctrine in European human rights law, which has no parallel in US law, is the means by which deviations from apparent requirements of the Convention are permitted by the Strasbourg Court. A margin that is "fairly wide" is very elastic, meaning that all but the most egregious privacy invasions will avoid condemnation if the purpose is to protect national security.

21. The Court has not yet considered cases arising from the Snowden revelations – there are several of them wending their way to Strasbourg challenging national laws, but they are unlikely to be decided for some time and may well be determined by application of the 'margin of

[21] See "*A Question of Trust*" (June 2015) Recommendations 42(b) and 44, p276-7
[22] *Weber* above, para 106

appreciation' for national security surveillance. Several cases have been considered by the UK's Special Intelligence Court in relation to GCHQ surveillance, the product of which is usually transferred to the NSA, and thus far no serious breach of UK law has been established - indeed, in one most recent case before the Investigatory Powers Tribunal, brought by **Privacy International**, it was decided that UK law permitting receipt of PRISM-collected data satisfied the "national security" exception in Article 8(2)[23]. In the meantime the UK government is proposing in its new *Investigatory Powers Bill* to permit collection of all phone metadata, whilst France has taken emergency powers which would permit generalised data collection, although prior to the Paris massacres I understand that its intelligence services had been given very wide powers, conferred merely by Ministerial authorisation.

European Practice.

22. For all that the eight safeguards listed in para 17 above may appear as "pillars" of European data protection, and thus denote the "high level" which should be used for the purposes of comparison with the US, the problem is that no state in Europe can claim to have all (in some cases, any) of them firmly in place. It would be illogical, and certainly unfair, to compare American surveillance practice with "European" safeguards that do not really exist in Europe. It would not be a "like with like" comparison, for example, to contrast the aspirational safeguards suggested in European case law with actual practice in the US, when European practice permitted by the 'margin of appreciation' doctrine in national security cases falls so far short of European ideals. The real

[23] And see, for example, "We must hack to fight terrorists" GCHQ admits" – *The Times*, 2 Dec 2015, noting a case currently being heard by the Investigatory Powers Tribunal.

question is whether data held in the US has similar (or better) privacy safeguards in respect to national security surveillance than the same data held in Europe.

23. The problem of identifying any consistent European practice in the area of national security surveillance was pinpointed very recently by the **European Union Agency for Fundamental Rights** in its report, "*Intelligence Services: fundamental rights, safeguards and remedies in the EU*". It concluded that "there is no uniform understanding of 'national security' across the EU"[24]. It explains that "The national security exemption provides a methodological challenge" for EU law because of its lack of scope and uncertain application to the *Data Protection Directive* with respect to cross-border data transfers which are transferred to intelligence services[25].

24. So far as the first (and most basic) pillar is concerned, the Council of Europe Commissioner for Human Rights has said that "*in many Council of Europe member states, bulk untargeted surveillance by security services is either not regulated by any publicly available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures*". According to this report only five states have laws applicable to Signals Intelligence intercepts, and in general "*national legal frameworks lack clear definitions indicating the categories of persons and scope of activities that may be subject to intelligence collection*"[26].

[24] Report, p10
[25] Ibid, p11
[26] Ibid p27

As for oversight,

"*There is no Council of Europe member state whose system of oversight comports with all the internationally or regionally recognised principles and good practices...*"[27])..."*Diversity in politics and legal systems has translated into a great variety of bodies that oversee intelligence services. EU member states have vastly different oversight systems*" [28]

As for remedies against surveillance abuses,

"*the remedial landscape appears ever more complex: the powers of remedial bodies are curtailed when safeguarding national security is involved*"[29].

25. These extracts illustrate the current failure of European States and courts to develop any coherent interpretation of the national security exemption in Article 8, other than to allow it to take the intelligence services outside the pillars of privacy protection. The Report demonstrates that where national security is concerned, the pillars remain largely unconstructed, and that it would be difficult to state a consistent European practice in relation to electronic surveillance for national security (as distinct from law enforcement) purposes. The Report notes that there have been few post-Snowden cases brought and none yet decided: "European" standards will be clearer when they are, in several years time. For the present, the comparative exercise

[27] Ibid p27
[28] Ibid p57
[29] Ibid p59

mandated by *Schrems* must be wary of any assumption that there is in Europe "high level" privacy protection against national security interception.

The US Position Today.

26. The Snowden revelations caused some concern in Europe, especially in Germany – a fact commentators put down to memories of the Gestapo, aggravated by the news that Mrs Merkel's mobile had been intercepted by the NSA. In America the implications of Snowden for Fourth Amendment rights was anxiously and angrily debated, and soon led to legislative and judicial reforms to protect the privacy of American citizens – and others.

27. The Snowden revelations began in June 2013, when *The Washington Post* and *The Guardian* revealed surveillance programmes, which had allowed the NSA access to the personal data of millions of American – and European – citizens.[30] The first legal ruling came in December when a federal Judge ruled in *Klayman v Obama* that bulk collection of American telephone metadata was significantly likely to violate the Fourth Amendment.[31]

> "I cannot imagine a more 'indiscriminate' and 'arbitrary' invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analysing it without prior judicial approval".

[30] The companies themselves were not complicit – see https://www.facebook.com/zuck/posts/10100828955847631

[31] (D. D. C. 2013) Civil Action No. 13-0881 (RJL)

This decision was vacated for procedural reasons but it showed US law as robust in action. Judicial review of governmental agencies is a regular and accepted aspect of US law, and of course the Federal Courts have more extensive powers under the Constitution to strike down legislation than courts possess in Europe. The judges of the FISA court have full judicial independence, which they exercise in approving or (albeit rarely) disapproving applications for sovereign intelligence warrants.

28. The President appointed an advisory Review Group, which in December 2013 released a 300 page report which recommended important changes to increase the privacy protections required in US surveillance programmes, both in relation to the generalised collection of "metadata" (telephone records) and to the law regulating security intercepts – FISA and its 2008 Amendment Act, and Executive Order 20333. It said that privacy advocates (specially vetted *Amicus* counsel) should be permitted to appear in the FISA court to oppose warrant applications, on Fourth Amendment (i.e. privacy) grounds. On 17 January, 2014, the President announced reforms based on the panel's report. He also – in terms I shall consider later – said that US surveillance programmes would henceforth have safeguards for foreigners, as well as for US citizens.

29. In February 2014, an independent US body – The **Privacy and Civil Liberties Oversight Board** (PCLOB) – issued two extensive reports. The first concluded that the bulk metadata programme was illegal and must be stopped. The second examined surveillance programmes conducted

under S.702 of the FISA Amendment Act, including PRISM, and concluded they were legal but needed further privacy protection, including protection for foreigner's personal data. Then the Second Circuit Court of Appeals ruled that the NSA's bulk collection of phone records was illegal, and called on Congress to act. It did, and on 2nd June 2015, by 67 votes to 32, the Senate passed the *USA Freedom Act* which prohibited bulk collection of US citizen phone records and which has just now come into force. In September of this year, the US Senate Intelligence Committee dropped a proposal to require social media companies to report any "terrorist activity" to government authorities.

30. One factual error made by the Court in *Schrems* – seemingly as a result of the 'facts' found by the Irish court – was to describe the PRISM programme as a bulk or 'generalised' data collection. This is not the case, and confuses PRISM with the bulk collection of metadata, also exposed by Snowden, which was ruled illegal by the Second Circuit Appeals Court and ended by the USA Freedom Act. As the second PCLOB **Report on the Surveillance Programme Operated Pursuant to Section 702 of FISA**[32] explains, PRISM "does not operate by collecting communications in bulk...it consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence".[33] What happens is that the government sends a selector, such as an email address or a key word, to an internet service provider, which is compelled to give all associated communications to the NSA. This is authorised by law – FISA and its

[32] July 2, 2014
[33] Ibid, p103

2008 Amendment Act, which brought in S702 under which PRISM commenced in 2009. S702 mandates 'minimalisation' procedures, approved by the FISA court, that govern agency use, retention and dissemination to other agencies of intercepted data. PRISM was closely examined by PCLOB, which concluded that its obtaining of foreign intelligence information "by using specific identifiers and subject to FISA Court approved targeting rules and multiple layers of oversight" fitted with the "totality of circumstances" test for reasonableness under the Fourth Amendment.[34] There is confusion in the ECJ judgement between 'bulk' or 'generalised' collection without safeguards – a feature of the metadata collection which Snowden exposed and which is now banned – and the PRISM programme. What must be put into the balance against European law and practice in the national security context is surveillance of foreigners conducted under S702 – a programme using 'selectors' to identify targets. This is not 'bulk' or 'generalised' collection, and is more akin to the "strategic monitoring" which was upheld by the European Court in *Weber and Saravia*.

31. In my judgement, as of today, it cannot be said that US law and practice on data privacy for European citizens in national security contexts is less than "adequate" – it is more than adequate compared to the treatment of their personal data under European law and practice under the 'margin of appreciation' granted in such context by the ECHR. It is not "essentially equivalent", but on the whole essentially superior, certainly when judged at this time after changes to US law and practice since 2013. The test that *Schrems* and Directive 95/46 mandate is whether an

[34] ibid, p9

"adequate level of protection" is afforded by the US, not to its own citizens, but to European citizens whose personal data on Facebook etc has been transferred to America. Do they have the same, or reasonably similar privacy rights under US law as they do under EU member states' laws?

Eurodata in America.

32. At the time of the Snowden revelations, foreigner's data on US servers had three important statutory protections, which still operate:

1. The limits on the scope of S702 surveillance, which must be confined to the collection of foreign intelligence information, (including protecting allies against international terrorism) and requires review and certification by the FISA court. This prevents, by law, the unrestricted collection of information about foreigners.

2. There are penalties applying to government employees who engage in improper surveillance – of foreigners as well as American citizens. Unlawful collection is not only a disciplinary offence, but could involve criminal penalties. Moreover, S702 specifically gives foreigners the right to a civil remedy if their data is mis-used – a matter that could come to light were it to be used, e.g. in a criminal proceeding or an immigration or extradition case.
3. There is a further statutory prohibition against improper disclosure of intercepted data, under 50 USC 1806. A federal employee would be liable to prosecution if personal data about foreigners were disclosed, e.g. in order to discourage them from exercising to free speech or in

order to disadvantage them for reasons of their race or religion or gender or sexual orientation.

33. FISA itself has some built-in protection for foreigners – they must be notified before their data is used in any court proceedings, so that they can obtain its suppression on grounds that it was unlawfully acquired. Moreover, they benefit from the minimalisation procedures applied to US citizen data, simply because it has been found impracticable to distinguish between the two categories.[35] Moreover, the requirement under EO12333 that intelligence agencies use "the least intrusive means feasible" applies to all intelligence gathering activities irrespective of the citizenship of the targets.

34. America has ratified the **International Covenant on Civil and Political Rights** which obliges it to care for the privacy of others as well as its own citizens[36], although it has not ratified the Convention protocol under which complaints may be heard by a Tribunal. Although signatories to this Treaty, and its Tribunal, have not agreed on how the UN privacy right is to be applied in national security cases, it is notable that this international right is being referred to, and taken into account, in the reports of US oversight bodies.[37]

35. Now, significantly, the US has the President's statement on 17 January 2014, extending privacy rights to foreigners. This is now part of Presidential Policy Directive (PPD)-28.

[35] See the PCLOB Report, p98-100

[36] See Article 17: "No-one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence...Everyone has the right to the protection of law against such interference".

[37] See, for example, PCLOB Report, p100.

"*All persons should be treated with dignity and respect, regardless of their nationality or wherever they may reside, and all persons have legitimate privacy interests in the handling of their personal information. US signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides*".

36. This came in Section 4 of a statement whose previous sections set out the "privacy pillars" – legal authorisation, legitimate purpose and collection only when necessary for national security. The intelligence agencies were directed to adopt data protection policies and procedures "to the maximum extent feasible consistent with national security... *to be applied equally to the personal information of all persons, regardless of nationality*". Moreover, "Personal information shall be disseminated only if the dissemination of comparable information concerning US persons would be permitted under Executive Order 12333".

37. This Presidential Directive requires every agency to report on adoption of these policies within a year. I have examined the new policy documents that have emerged from the NSA, CIA, FBI, Homeland Security and Department of Energy, and they all make appropriate extensions of privacy safeguards to non-nationals.

38. The President also promised reforms to place additional restrictions on Section 702 of FISA, which permits targeted surveillance of US citizens

with some privacy safeguards which do not apply for non-US persons, although as explained above, they do have a right to seek judicial remedies (a right limited in practice unless they are notified eventually that they have been under surveillance). This means that the introduction of "Special Advocates" in FISA courts, reminding the court of the promises of PPD-28, is a particularly valuable and realistic safeguard (although interestingly it is not one of the privacy 'pillars' thus far erected by European law). Perhaps the most important aspect of the reforms will be oversight mechanisms that now, avowedly, ensure fair treatment for foreign data: the PCLOB has extensive subpoena powers to check targeting appropriateness and minimalisation procedures and the NSA, for example, has an Inspector General, a General Counsel and a Civil Liberty and Privacy Director, all required to "keep an eye" on fair treatment of foreign data.

39. PPD-28 is not law, even though it does operate as a directive to the spying agencies which the President commands, i.e. the NSA, CIA and FBI. In the case of the NSA, for example, it is adopted in regulation USSID SP 0018, and its rules may be deviated from only in "uncontemplated or extraordinary circumstances". No data relating to a foreign citizen should be held for more than five years. The first Annual Report on Implementing PPD-28 expresses the Intelligence Community's support for ensuring protections for foreign citizens, hence its "work with Congress to give citizens of designated countries (EU countries may be 'designated') the right to seek judicial review, together with damages", where their personal data has not been adequately protected. These steps are all in the direction of greater privacy

protection for EU citizens, even if such citizens are not singled out for equivalent treatment and are not, as foreigners, fully protected by the statute law which creates additional legal rights for Americans.

40. This is, of course, the problem: PPD-28 does not extend *legal* rights and expressly states in Section 6 that it "is not intended to, and does not, create any right or benefit, substantive or procedural..." Moreover, the equal application of the law to foreigners through administrative practice is "to the maximum extent feasible" and "consistent with national security" – clauses that could permit some derogation from the promise of equal treatment. However, for the purpose of applying the 'essential equivalence' test, it does not matter that US law treats EU citizens differently, so long as it treats them in a way that gives them protection that at the end of the day is consistent with the protection they receive in Europe. The statements of principle in PPD-28 are more definite than those in European surveillance laws.

41. European courts may be prejudiced against a finding of "essential equivalence" by virtue of the simple fact that European data relies, for protection in the US, mainly on administrative practice. Although the Directive against discrimination is now reflected in the rules and practices of all US surveillance agencies, there are still doubts over whether the new safeguards are "safe" – see the title of a recent article in the *Harvard Law Review, "American Surveillance of non-US persons: Why New Privacy Protections offer only Cosmetic Change".*[38] This is a somewhat academic discussion, and ignores the reality of the change of

[38] Daniel Severson. *Harvard Law Review,* Vole 56 No 2, Summer 2015, p465

culture in the agencies. It notes the long-standing policy of applying these protections to residents of UKUSA partners (including UK residents) but denying them to citizens of European allies. The policy has now been extended, by presidential fiat, to all foreigners. A more detailed and authoritative analysis of the post-Snowden reforms to the apparatus of national security surveillance in the US is found in Professor Peter Swire's Paper, "*U.S. Surveillance Law, Safe Harbour, and Reforms since 2013*"[39] He demonstrates no less than twenty-four reforms that have enhanced privacy protections, many of which will benefit EU nationals whose data is transferred, and he exposes the mistakes made by the Advocate-General in *Schrems* which led to the EU Court's mischaracterisation of the PRISM programme. Although I consider his confidence in the US system may in certain respects be over-optimistic (especially in relation to the FISA court, which has in the past been over-secretive and under-critical of government spying programmes) there is no doubt that the reforms of the past two years have provided a more effective oversight of national security surveillance than exists in any country in Europe.

42. PPD-28 is not law and the 'safeguards' for foreigners are set out – in some detail – by way of administrative rules and arrangements circulated in all surveillance agencies. This provides a level of practical protection for European data, which may well ensure that it is better safeguarded as a practical matter than data in Europe, where surveillance agencies do not usually publish their internal surveillance guidance. Would a European court be prepared, in conducting an

[39] December 17, 2015, Published by The Future of Privacy Forum

"essential equivalence" exercise, to take such arrangements into account? The recent decision of the Investigatory Powers Tribunal in *Liberty v GCHQ* does so, finding that administrative "arrangements" within the organisation, although they had not been made public and did not constitute 'law', provide sufficient safeguards in practice to satisfy Article 8. These internal rules[40] were "below the waterline", so it is difficult to see how a European court could ignore "above the waterline" rules and arrangements in the US that are intended to implement a presidential directive and which are made available to the general public – and can be enforced by disciplinary procedures when breached and where any such breach is deterred by the prospect of criminal penalties. Since US surveillance practice in a national security context is more transparent than that obtaining in most European states, this fact must also be put into the balance in favour of the 'adequacy' of US protection.

43. In sum, looking at the present position in relation to national security data collection in the US and comparing it with the European equivalent, Europeans have more real protection in the US than they do at home. For example, Europeans have very little protection against national security surveillance from the ECHR, given its 'fairly wide' margin of appreciation doctrine. European law does not necessarily require court approval for it, and European governments have no clear prohibition against spying on foreigners. In some respects, US standards are not

[40] IPT/13/77 H, 5 December 2014

"essentially equivalent" but effectively superior. As Timothy Edgar comments in *Foreign Affairs*[41]

> "*The US has an impressive array of privacy safeguards, and it has even imposed new ones that protect citizens of every country*. *Despite their weaknesses, these safeguards are still the strongest in the world...the US government should urge other countries to follow its lead*".

44. Although it is true that the European Union has more detailed rules concerning the processing of ordinary data than the US, in respect to intercepting and procuring data on national security grounds it offers very little protection, and these protections are (in France and the UK) likely to reduce even further. It is in the context of the national security exemption that the *Schrems* exercise must be conducted. It does not call for some general comparison between laws relating to privacy or to data protection generally: it requires a more sophisticated assessment of the adequacy of the law and practice relating to secret surveillance on the grounds of national security, taking into account the factors listed in Article 25(2) of Directive 95/46 which include the purpose of the operation (e.g. gathering information relevant to international terrorism), the nature of the third country (an ally in NATO, and in combating terrorism) and the "professional rules and security measures which are complied with" by virtue of PPD-28 and its associate regulations.

[41] April 2015, "*The Good News about Spying"*

45. In this respect, European courts cannot ignore the importance of the US intelligence agencies to their own security. International terrorism is a blight in Europe, as the Paris and Madrid atrocities demonstrate, and information from the NSA, which is usually volunteered to its European counterparts, may save lives. Article 8 expressly permits derogation when this is necessary in the interests of national security and public safety. The PCLOB report anxiously interrogated the value of PRISM: it concluded

> "*The programme has proven valuable in the government's effort to combat terrorism – monitoring terrorist networks under S702 has enabled the government to learn how they operate and to understand their priorities, strategies and tactics... (and) to identify previously unknown individuals who are involved in international terrorism and it has played a key role in discovering and disrupting specific terrorist plots aimed at the US and other countries".*
>
> In the present climate I have little doubt that a European court would find that this meets the "public safety" and "national security" exemptions in Article 8(2).

46. So I am satisfied – and I think the Irish Data Protection Commissioner should be satisfied – that although the national laws in Europe across the continent could be characterised as insufficient in meeting Charter standards, US law and practice post PPD-28 is "adequate" enough – sufficient, at least, to prevent any reversion to the secret world exposed by Snowden in which personal metadata was "hoovered up" without

court or any other lawful authorisation and without any prospect for redress. I am reinforced in this view by the history and tradition of a country with constitutional protection for privacy long before European countries; with elected representatives prepare to investigate through congressional committees the conduct of the intelligence services (which are in any event obligated by statute to keep them "fully and currently informed" of all intelligence activities); with a media that is more than willing to expose secret agencies, and powerful NGOs, like the ACLU, which take legal action when privacy rights are infringed on grounds of national security. Of course, developments in the EU and in the USA must be monitored, and the question of "essential equivalence" needs to be considered from time to time, but at the present moment I consider that US privacy protections in respect of data sought for national security purposes are, in reality, at least equivalent to such protections in the EU.

Alternative Approaches.

47. *Schrems* has directed continued investigation by the Irish Data Protection Commissioner, and Facebook may well wish to be heard in this investigation so as to advance the contention set out above, and/or to do so in the course of continuing discussions with the Commission, pointing out that the US now has a developed and sophisticated system of protecting the personal data of Europeans from unnecessary national security interception which achieves the basic Charter objectives and does so more effectively than the law and practice of European states. There are, however, ways of legally derogating from Article 25 principles

of Directive 95/46, and they are set out in Article 26. Under 26(a), data may be transmitted to an 'inadequate' third country if "the data subject has given his consent unambiguously to the proposed transfer". No doubt the great majority of Facebook members would happily consent to the transfer of their data to US servers were they asked directly and clearly, and provided with the relevant information about PPD-28 and the post-Snowden protections (their data may not be safe from GCHQ interception, but that is another issue). This would doubtless be seen by privacy campaigners as a circumvention of the court decision, but it would be a circumvention that the Directive expressly permits.

48. Another alternative that has been suggested is for Facebook – together perhaps with other companies affected by *Schrems* – to set up its own independent oversight body to keep US law under review, to apply for representation at FISA hearings, to provide legal assistance for complainants and for those with a case for judicial remedies. This might be built into a "Safe Harbour II", but would require the co-operation of US authorities to work effectively. It would be important, as a matter of principle, not to involve Facebook itself in making any judgement on its members' personal data.

Conclusion.

49. In my opinion, the "adequacy" of US privacy and data protection law compared with European law must be considered in the specific context of national security interception. There is no 'European' law to be compared against: the EU itself has no jurisdiction or competence on questions of national security. National laws vary greatly, and ECHR

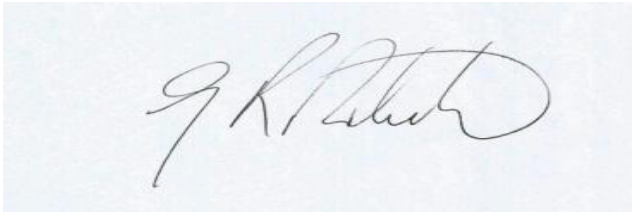
decisions on Article 8 mainly concern targeted surveillance. I do not agree with suggestions in *Schrems* that bulk data collection is itself unlawful: it may be necessary e.g. to track down jihadis or to interpret past events that have led to atrocities. It is, in my opinion, lawful to the extent that there are sufficient safeguards to satisfy Article 8, and these may include judicial warrants, procedures for speedy removal and destruction of irrelevant personal data, remedies against abuse and so on.

50. Although European law on data processing is more developed than US law, that country has a long history of balancing Fourth Amendment rights against the needs of law enforcement and national security: its procedures are much more transparent and its oversight much more formidable than that which obtains in European states. Citizens in the US are better protected in this area of national security interception than citizens in Europe.

51. However, the ultimate question is whether the personal data of European citizens is adequately protected in the US – and until the Snowden revelations, it was not sufficiently protected - unlike the personal data of citizens of UKUSA partners (including, from Europe, only the UK) which was protected as a matter of policy, although not of law. The exclusion of other EU countries from statutory protection rankles and might prejudice a European court against finding "essential equivalence", although on close study of the regulatory foreground at intelligence agencies it is evident that PPD-28 foreshadowed an end to disparate treatment and that all foreign data is now being protected to a

considerable extent by administrative rules and arrangements which implement that directive without actually bestowing enforceable legal rights on foreign data subjects.

52. In my judgement, given the weakness of European legal protection against national security surveillance, the growing acceptance by governments (certainly in the UK and France) that bulk collection of data is necessary to deal with Islamic extremist threats, and the historic deference by the judiciary in Europe to national security interests, it can be said on a practical level that the data of Europeans receives "essentially equivalent" protection under US laws and oversight arrangements and the decisions of independent judges at the FISA court, together with the practices mandated by PPD-28, when and after it is transferred to servers in America.



Geoffrey Robertson QC

Doughty Street Chambers

14th January 2016