December 2015

Big data, Big Brother?

How to secure Europeans' safety and privacy

By Camino Mortera-Martinez

CENTRE FOR EUROPEAN REFORM

OPEN SOCIETY FOUNDATIONS

Big data, Big Brother?
How to secure Europeans' safety and privacy

By Camino Mortera-Martinez

★ Terrorism and organised crime are a serious threat to Europe, as the recent attacks in Paris show. The European Union is better placed to deal with trans-national crime and terrorists moving across borders than individual member-states. To face this growing threat, the EU needs to adopt security measures. Some of these measures (such as the use of data to trace and track how terrorists are financed, how they travel and how they communicate) have far-reaching implications for citizens' privacy.

★ As it tries to find more effective ways to combat terrorism at the European level, the EU has been struggling to find the right balance between privacy and security. There are two main reasons why: the EU's institutional and legal framework for dealing with security issues is inadequate; and debates on security and privacy are distorted by Europe's love/hate relationship with the US, which extends to American multinational companies. The European Parliament has been blocking important security legislation, and the Snowden revelations have damaged trust between Europe and America, threatening the operations of US companies in Europe. But the EU needs to protect its security and ensure that citizens' rights are respected. The following proposals would help it to do so:

  ★ The European Parliament needs to have access to confidential information, if the EU wants to overcome the current gridlock on security measures. For that, MEPs need to have security clearance. Security-vetted MEPs could be part of a special sub-committee that would be responsible for examining counter-terrorist measures.

  ★ A recent ruling by the European Court of Justice has declared that the 'Safe Harbour' agreement regulating transatlantic data flows is invalid. The EU and the US should consider a legally binding bilateral treaty which would regulate these flows. They should also adopt measures, perhaps in the form of a treaty, to ensure that citizens on both sides of the Atlantic are protected from unwarranted surveillance. Transatlantic agreements in the field of commercial data transfers and surveillance will not happen immediately, but there are reasons to be optimistic: the EU and the US have been working hard to find a common ground to restore trust in transatlantic data flows, as shown by recent agreements in the field of data transfers for criminal investigations.

  ★ Transatlantic relations would also benefit from extending Europol's role in intelligence matters. Europol should become the main EU interlocutor with America on intelligence sharing. For this, the EU will need to convince some national intelligence agencies, who feel more comfortable working on the basis of bilateral agreements rather than pooling information at the EU level. But as proved by the recent attacks in Paris, European co-operation in intelligence sharing is vital to fight against the growing threat of foreign fighters. Europol is best placed to act as a hub for European intelligence, and as the main interlocutor with third countries such as the US.

  ★ Encrypting digital communications helps to safeguard citizens' privacy and to restore consumers' trust in online service providers. But some European governments, like France or the UK, are now calling for a ban on encryption. They should think again: the EU and its member-states should support encryption, albeit with limitations. Law enforcement agencies should

have access to communications when they need it – and certainly in times of emergency, following terrorist attacks. Internet companies must be able to 'crack' encrypted data and pass it to law enforcement.

★ The Union should also make cross-border requests for information easier, by reforming Mutual Legal Assistance Treaties that regulate trans-national requests for information within the EU. The EU and the US should simplify the ways they share information, by reducing the number of overseeing agencies, and moving information requests onto a web-based platform.

On Friday November 13th 2015, three suicide bombers blew themselves up outside Paris' Stade de France, killing one passer-by. Simultaneously, gunmen attacked four restaurants and cafés in the city's trendy 10th district, killing 39 people and injuring many others. A suicide bomber detonated a vest inside another café, injuring 15 people. Only fifteen minutes later, heavily armed terrorists opened fired inside Paris' 'Bataclan' concert hall, killing 89. In total, 129 people died and 352 were injured. The Paris attacks were the latest in a string of jihadi attacks on European soil. Coinciding with the one-year anniversary of the establishment of the Islamic State's (IS) 'caliphate', in June 2015, French Islamic terrorist Yassine Salhi decapitated his employer and injured two people at a factory in the French Alps. In February 2015, Danish-born Omar Abdel Hamid El-Hussein, claiming to be an IS fighter, killed three people in Copenhagen. One month before, in January 2015, Cherif and Said Kouachi, two French brothers identifying themselves as al-Qaida members, killed 12 people in the office of satirical magazine *Charlie Hebdo*. Five more people were murdered the next day in related attacks carried out by Amedy Coulibaly, who was also an IS affiliate. In May 2014, French citizen Mehdi Nemmouche opened fire at the Jewish Museum in Brussels, Belgium, killing four people.

The terrorists involved in the Paris attacks of November 13th were later discovered to be French and Belgian citizens, and the massacre was allegedly organised by Belgian national Abdelhamid Abaaoud, killed two days later in a police raid in Saint-Denis, north of Paris. Abaaoud is thought to have been travelling back and forth from the Schengen area to Syria without being detected. Of the eight terrorists carrying out the attacks, seven died and one, Salah Abdeslam, fled, allegedly to Belgium. Lars Vilks, a Swedish artist famed for drawing cartoons of Mohammed, was El-Hussein's main target: he had organised an event on free speech at the café where the shooting took place. The Kouachi brothers were included in a US no-fly list that was never shared with European authorities. Both the Kouachi brothers and Coulibaly reportedly acquired their arsenal near Brussels' main train station and then brought the weapons into France. Coulibaly's wife is thought to have fled to Syria via Madrid, without being stopped. Nemmouche was arrested in Marseille, where he had arrived after taking a bus from Amsterdam via Brussels. His arrest was coincidental, as his bus had been stopped for a random drugs search: Dutch, French and Belgian police and customs officials keep a close watch on the route, which is a favourite of traffickers smuggling drugs from Amsterdam to the South of France.

After both terrorist attacks in Paris – on *Charlie Hebdo* and on November 13th, the EU's justice and home affairs (JHA) ministers called for increased security co-operation. Islamic terrorism has been a global threat for more than a decade. But the radicalisation of EU citizens, who can freely move around the continent, creates a new problem, which requires an EU solution. The absence of European co-ordination leaves security gaps that can be dangerous for all member-states, as the latest events in Paris show. The challenge facing the EU is daunting because terrorism comes in many forms, from attacks which are carefully planned and directed from overseas, to local conspiracies, to 'lone wolf' attacks inspired by internet propaganda. The EU and its member-states will have a better chance of dealing with these diverse threats successfully if they unite their efforts, and if they work with international partners, like the US, who face similar problems.

It is difficult to know how big the scale of the terrorist threat really is, and in fighting it, the EU and its member-states are using tools which have an impact on citizens' privacy. The balance between privacy and security is delicate. It involves judgements about the government's need for surveillance; a citizen's right to privacy of communication, even if that means encrypting data;

and it must also take into account the (inconsistent) attitudes that people have towards sharing data with the government and on social media. Citizens do not want governments snooping on them, yet they seem happy to publish pictures of their birthday parties and revelations about their personal lives on Facebook. Companies want to help governments catch terrorists, but they still need to maintain business models which depend on customers thinking that their data is safe with them. Meanwhile, nobody outside the intelligence and law enforcement world knows how many plots have been foiled thanks to the collection of private data.

This policy brief looks at the trade-off between privacy and security; assesses the deficiencies of the EU's approach to privacy and security, including its love/hate relationship with the US; and recommends ways to fix the problems.

Privacy versus security: The great trade-off

Data is increasingly valuable. Most of us (terrorists included) use credit cards, phones, tablets and computers. The volume of data that can be extracted from everyday activities such as a phone call or a credit card transaction is unprecedented. This data can be used for a variety of purposes, from marketing to fighting terrorism, and both businesses and governments have started to exploit people's data. After the terrorist attacks of September 11th 2001, states increased their surveillance activities. Government surveillance programmes range from directly monitoring phone calls, text messages or emails, to collecting 'metadata' – patterns of telephone calls and websites visits – to tracing suspicious financial transactions. Governments implement two types of surveillance programme: they collect data on identifiable individuals about whom they are suspicious (targeted surveillance); and they trawl through all available data, looking for patterns that might ultimately lead them to find someone doing something dubious (untargeted surveillance or bulk data collection).

There is, however, a clear trade-off between privacy and security. The question is whether people think that giving up some privacy for the sake of security pays off, and if so, where they want to draw the line. Few people would complain when their bank informs them that it has stopped someone conducting a fraudulent transaction in a far-away country with their credit card details; but to do that the bank needs to know (at least) that a person is not on business in the country concerned, or that they are not in the habit of buying, say, expensive jewellery.

Technologies tracing and tracking people's movements and behaviours are continuously deployed to improve citizens' security. But people seem to be generally less concerned about private companies (notably online services providers, such as social media or search engines) collecting and using their data, than the state doing so.

One reason is that many people do not see their data as a valuable currency, and do not know that they are paying for seemingly free internet services with their data.[1] A recent study by the University of Pennsylvania suggests that fatalism also plays a role: according to the researchers, Americans have given up on their data ever being private again, and have resigned themselves to providing it to a myriad of online providers.[2]

> *"The question is whether people think that giving up some privacy for the sake of security pays off."*

In some European countries, particularly those with a history of authoritarian government, the general public seems more worried about the use of personal data by the state. For one thing, while citizens may see the value of giving up their privacy in exchange for online services, they find it harder to grasp what they get in return for the state's use of their data. Intelligence services may regularly tell them that data-gathering has helped to foil a number of terrorist attacks. But the specific ways in which the authorities stop plots remain secret, for obvious reasons. With the development of technology, it has become more difficult for citizens to understand when the state is encroaching on their privacy without justification. Whereas citizens feel that they can always cut their ties with online service providers, if need be, some consider that there is no way for them to 'terminate' their contract with the state – and prevent the authorities from gathering their data. And there is currently no way of knowing how much data the state has and for what purposes it is used. There is also no 'opt-out clause'.

From mass surveillance to encryption

Popular discontent with government snooping reached its peak when Edward Snowden exposed the US government's secret mass surveillance programme. Snowden, a former contractor with the US National

1: According to recent research by the Pew Research Center, half of online users in the US do not even know what a 'privacy policy' is – a clear sign that people hardly realise the 'costs' of signing up to social media.

2: Joseph Turow, Michael Hennessy and Nora Draper, 'The trade-off fallacy: How marketers are misrepresenting American consumers and opening them up for exploitation', University of Pennsylvania, June 2015.

Security Agency (NSA), leaked documents to the press showing that the US administration was sweeping up data on "virtually every telephone call made to, from or within the United States".[3] Snowden also revealed the existence of PRISM, a programme that allows the NSA to collect data from some big internet companies, including Google, Facebook and Skype. The leaked documents also showed that the British Government Communications Headquarters (GCHQ) was gathering bulk data through its TEMPORA programme.

These documents showed that governments were monitoring citizens' activities with the – sometimes involuntary – help of online service providers. The revelations made people question private companies' data privacy policies and their role in the fight against terrorism. Some of the industry's major players, worried about the effect that the Snowden scandal would have on their corporate reputations, and, eventually, on their turnover, began pushing for a blanket right to encrypt all their communications.

Encryption technologies allow companies to encode users' data so that they can only be accessed by recipients approved by users themselves. Technologies facilitating 'anonymity' can also protect users' privacy. These technologies are used to disguise users' identities and their digital footprint – the sites they have visited and the communications they have made.[4]

Online services providers, such as Google, Facebook or Microsoft, think that encryption is the best way to protect consumer privacy. Some go as far as to implement encryption codes they cannot break themselves. For example, Apple has encrypted data in its latest iPhone so that nobody, including Apple itself, can access it – even if asked to do so by law enforcement agencies. The table below shows how widespread encryption has become.

Table 1: Who is encrypted?

Source: Financial Times

Service	Company	Monthly active user numbers	Encrypted from
WhatsApp	Facebook	800m	November 2014
Gmail	Google	900m	March 2014
Yahoo Mail	Yahoo	225m	January 2015
Facebook	Facebook	1.4bn	July 2013
iMessage	Apple	450m	June 2011
Face Time	Apple	450m	June 2010
Skype	Microsoft	300m	August 2003

Encryption and anonymity are not only used for protecting consumers' data. They can also help whistle-blowers, dissidents and other at-risk individuals to exercise their fundamental rights. The 'darknet' – websites which use anonymity systems to conceal their users' identities – can "help citizens to protect their security and privacy and to circumvent censorship".[5] But anonymity technology can also help paedophiles, drug dealers and other criminals who use the 'darknet'.

European governments are calling for a ban on encryption, especially after the latest attacks in Paris. They argue that encryption hinders the fight against terrorism and organised crime, and puts citizens' security at risk. British prime minister David Cameron recently said that the government must be able "to read someone's letter, to listen to someone's call".[6]

Online service providers argue that encryption is the only way to protect consumers against malicious breaches of their privacy. But encryption keeps government out of the citizen's personal affairs, whether or not that business is legitimate. In the great trade-off between privacy and security, privacy activists have found unexpected allies in US technology companies.

3: Josh Gerstein, 'Democrats split sharply on NSA call-tracking program', *Politico*, October 2nd 2013.
4: David Kaye, 'Special report on encryption and anonymity', United Nations Office of the High Commissioner of Human Rights, May 22nd 2015.
5: Parliamentary Office of Science and Technology, 'The darknet and online anonymity', Houses of Parliament, March 9th 2015.
6: Nicholas Watt, Rowena Mason and Ian Traynor, 'David Cameron pledges anti-terror law for internet after Paris attacks', *The Guardian*, January 12th 2015.

Transnational problems need transnational solutions: Privacy versus security at the EU level

The latest attacks in France and Belgium show how easy it is for terrorists and other criminals to move around the EU and to communicate with each other across borders. It does not make sense for terrorists to be able to operate more freely than law enforcers. EU member-states and the Commission need to work together.

The EU has been working on measures to counter cross-border terrorism. The Passenger Name Records (PNR) directive would oblige air carriers to give European governments data on the itineraries, contact, payment and other details of passengers flying into or out of the EU. But the European Parliament has blocked it since 2011 and has only recently allowed negotiations to be restarted with the Council of Ministers. Under the Terrorist Finance Tracking Programme (TFTP), European citizens' financial data is sent to the US by the Society for Worldwide Interbank Financial Communications (SWIFT), a Belgian-based company that is at the heart of most international bank transfers. Both measures are based on the collection of personal data and thus have an impact on citizens' privacy.

While pursuing its important security goals, the EU needs safeguards that help it to balance privacy and security. But finding common ground on privacy issues at the EU level is far from easy. European countries have very different approaches to privacy. Citizens from post-authoritarian member-states (such as the former Warsaw Pact countries) are more wary of the state's intrusion in their private lives than those of long-standing democracies such as France. Those living in countries with a history of terrorism (such as the UK, Spain or even Italy) tend to be less suspicious of the state's use of their data. These differences may explain why Germans are so preoccupied with data protection while Britons are relaxed about being monitored everywhere by closed-circuit television.

As it tries to find more effective ways to combat terrorism at the European level, the EU has been struggling to find the right balance between privacy and security. Besides different national attitudes to the issue of privacy, there are two main reasons why this has been difficult. First, the EU's institutional and legal framework is complicating security reform; and security and privacy debates are distorted by broader tensions between Europe and the US.

The European Parliament and the Council: It's complicated

Since the Lisbon treaty entered into force in 2009, both the European Parliament and the Council of Ministers have had competence over justice and home affairs policy. By extending the Parliament's role in this area, the treaty aimed to improve the democratic oversight of security measures at the EU level. It is not clear that this has succeeded.

Since 2009 privacy and security have become some of the most controversial areas of EU policy-making. This is mainly due to serious misunderstandings between the Council and the European Parliament. It became apparent that the two institutions would have problems working together when the Parliament rejected the first EU-US TFTP (or SWIFT) agreement, in 2010, because of privacy concerns. The Parliament and the Council of Ministers also had serious disagreements over the EU-US PNR agreement, although the Parliament eventually approved it in 2012. Their differences over an intra-EU PNR system persist.

> *"The European Parliament needs to understand the implications of the security measures it is supposed to adopt."*

The European Parliament argued that the usefulness of both programmes did not justify the intrusion into people's lives. The Council, the Commission, Europol and the US disagree; in their view, TFTP has helped dismantle a number of terrorist plots. Europol, the EU's police agency, estimates that overall, more than 7,300 intelligence leads have been generated by TFTP since it went into force. The US government, the European Commission and the Council of Ministers have repeatedly emphasised that passenger data transmitted under the EU-US PNR agreement helped governments to foil plots and arrest wanted terrorists. High profile examples include New York City subway bomber Najibullah Zazi, Times Square bomber Faisal Shahzad, and Mumbai plotter David Headley.

When it comes to security matters, the Council and the Parliament do not trust each other. The Parliament feels that the Council patronises it, and Council officials see the Parliament as irresponsible.

One of the main issues at stake is access to information. The European Parliament needs to understand the implications of the security measures it is supposed to adopt. Threat assessments are vital to help it do so. But national security services are responsible for gathering the information needed to make threat assessments, and they are reluctant to share it with Europol and the Parliament. Since the EU does not have intelligence competences, national security services think they should retain control over the information they share, and choose who to share it with. The Parliament, in turn, finds it difficult to make informed decisions on measures which could restrict civil liberties when it has not seen the necessary intelligence.

The European Parliament is supposed to provide democratic oversight of privacy-invading measures such as TFTP or PNR. But it is failing to do so because it does not receive enough information, and because it lacks a satisfactory way of working with the Council on this issue.

Rows over security measures are often more about institutional power than the protection of citizens' interests. Until 2009, the Council alone took decisions on JHA matters. Before the Lisbon treaty entered into force, the Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE, which leads the Parliament's work on security) had little power. Knowing that their behaviour did not matter, LIBE members tended to adopt radical positions. LIBE's lack of pragmatism and the Council's historical reluctance to give up powers in the security field have complicated negotiations.

Without European co-operation on law enforcement and data sharing, the safety of 500 million Europeans is compromised. Because EU co-operation remains weak, national law enforcement services need to rely on bilateral agreements to find out whether a terrorist has flown from France to Latvia, whether they have moved money from Luxembourg to Malta, or whether Slovakia has useful data on a suspect that the UK is not aware of. Criminals know this and so exploit the system's deficiencies – as shown by the November attacks in Paris and the events that followed. Whereas some member-states work closely together to combat terrorism – for example, France and Spain have been doing so to defeat the Basque separatist group ETA for three decades – others do not – communication between France and Belgium, for example, seems to be surprisingly scarce. The EU needs to build a system that ensures a uniform level of protection across Europe and makes law enforcement easier.

Without some method of improving communication between Parliament and Council, the EU is in for several more years of unnecessary problems and arguments. And that is in no one's interest. Certainly not that of citizens, but equally not that of the Parliament's: the EP's role as the primary source of democratic input into EU law-making is routinely called into question because of its perceived inability to live up to its new responsibilities. This will not change unless the Council shares more information with the Parliament.

A single market in security?

A fragmented approach to security is not only bad for Europe's safety, but also for Europe's economy. The single market has been one of the main drivers of European integration. The rationale is simple: trade is easier in an area where standards and rules are harmonised to a certain degree.

What is true for the single market is also true for security. Private companies have to bear much of the burden of implementing the EU's security strategy. Banks, airlines and online service providers prefer a single set of security measures at the EU level rather than 28 sets of national rules. It is easier, and cheaper, if they only have to abide by one set of standards. And a harmonised system reduces the risks of legal loopholes that criminals can exploit.

"A fragmented approach to security is bad for Europe's safety and also for Europe's economy."

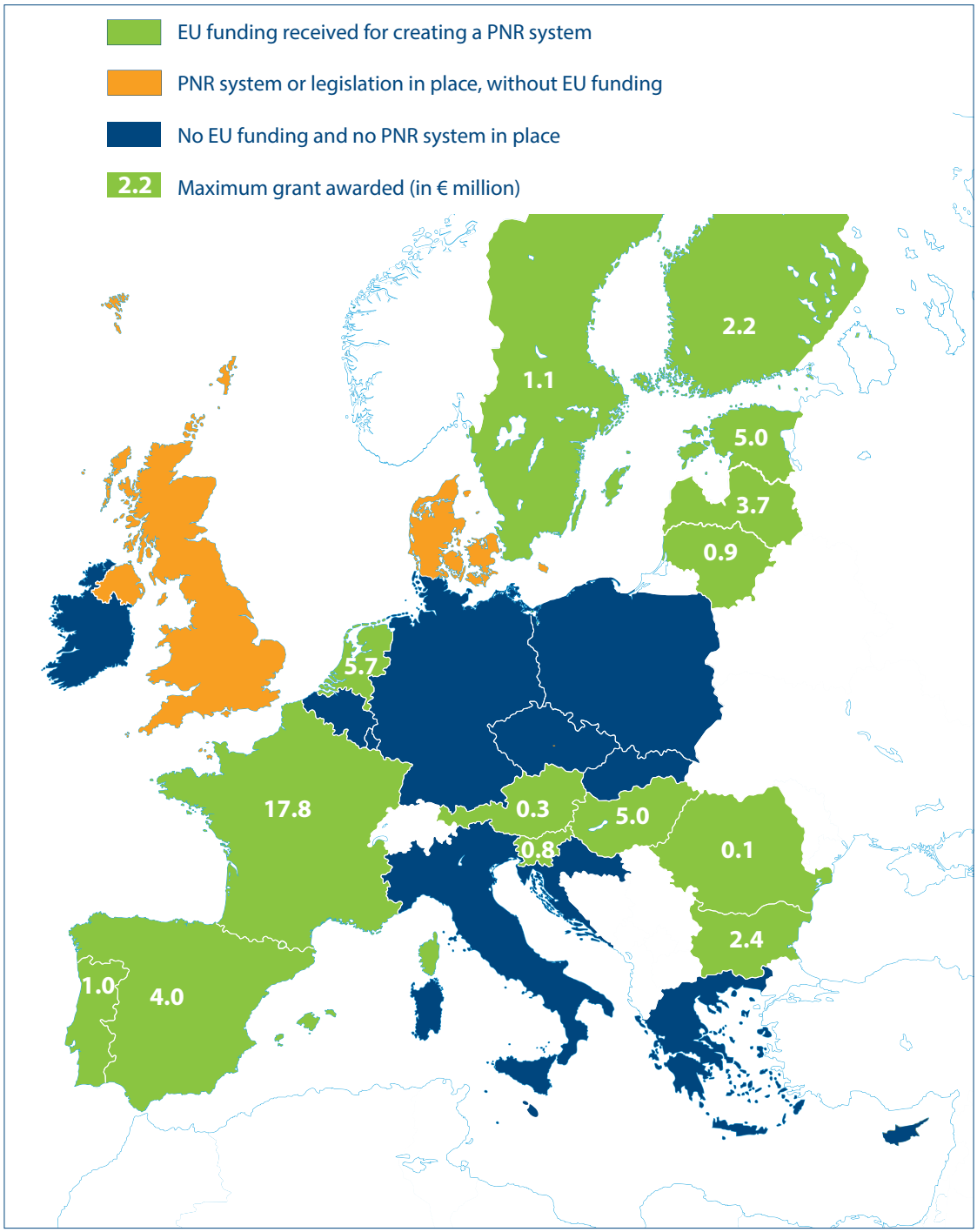
Even with a single framework across the EU, compliance with regulations will be expensive. If the EU decides to establish a European Passenger Name Record (PNR) system, airlines will need to have the necessary equipment and human resources to operate it. Likewise, EU rules combatting terrorist financing require banks to keep track of their clients' movements. Online service providers, like Google or Facebook, are required to hand over information to law enforcement authorities, when requested. They are also obliged to monitor and remove content that may be illegal (such as 'glorification of terrorism' material). Twitter has shut down accounts linked to alleged members of the Islamic State, while graphic images from that organisation's most violent crimes have been deleted from YouTube.

A recent revision of the directive setting up the EU's Advance Passenger Information (API) system showed how important common standards are. This directive required airline carriers to transfer passenger data to the authorities of the member-state of destination, but is much more restricted in scope than a PNR system–. One of the issues flagged was how expensive and technically difficult it was for air carriers to transmit API data to different member-states in the absence of a single set of standards agreed by the EU and the International Civil Aviation Organisation (ICAO).

In absence of an EU PNR system, the European Commission has made €50 million available to finance national PNR systems. Currently, there are 16 different PNR systems in Europe, 14 of which have been financed by the EU (the UK and Denmark have funded their own). Twelve member-states do not have schemes to allow air carriers to transfer PNR data to law enforcement authorities. The map below shows the fragmentation of PNR systems across the EU.

Figure 1: PNR systems in the EU

Source: European Parliamentary Research Service



With or without you: Privacy and security in the transatlantic context

While America and the EU are long-time allies, their different approaches to privacy and data protection have made transatlantic security co-operation far from straightforward. The European Parliament has been a particular complicating factor in negotiations with the US on counter-terrorism measures. From TFTP to PNR, to the Snowden revelations, the Parliament has never been shy of criticising America's counter-terrorism proposals. The US does not need to conclude agreements with the EU as a whole: internal security is still mainly in the hands of member-states, so if transatlantic negotiations on security issues fail, the US can always resort to bilateral agreements with EU member-states. But this would contribute to a further fragmentation of Europe's security measures.

The Parliament's suspicion of the US predates the Lisbon treaty. Before the attacks of September 11th 2001, the European Parliament criticised a US-spy scheme known as 'Echelon'.[7] The Parliament concluded

7: Charles Grant, 'Intimate relations: Can Britain play a leading role in European defence – and keep its special links to US intelligence?', Centre for European Reform, April 2000.

that 'Echelon' was not only an illegitimate system of surveillance, but that it had also facilitated cases of industrial espionage against European companies. After 9/11, the Bush administration's 'war on terror' did nothing to improve relations. In 2001 and 2002, privacy concerns were at the heart of difficult negotiations between Europol and the US over sharing strategic and technical information. Different approaches to privacy and security also slowed the negotiations of the 2006 agreement between the US and Eurojust (the EU's agency for co-ordinating the work of national judicial authorities) that facilitated co-operation in the fight of transnational crime, including terrorism.[8]

America and Europe have some differences in their approach to data protection, but the gap in citizens' attitudes to privacy is narrower than it appears at first sight. This is particularly true in the wake of the Snowden revelations. According to a survey conducted by the Pew Research Centre in early 2015, 88 per cent of Americans consider that "it is important not to have someone watch or listen to them without their permission."[9] By contrast, 81 per cent of Europeans say it is important for them to know who has information about them, and 79 per cent want to make telephone calls without being monitored.[10]

Citizens' attitudes towards privacy and security may not differ as much, but America's and the EU's legal approaches to protecting privacy are very different. The EU has a consolidated body of laws regulating data privacy, which are currently being reformed. The Parliament and the Council are negotiating both a general data protection regulation, which will replace the current directive that dates back to 1995, and a new directive on the protection of data in the context of criminal investigations and law enforcement. Article 8 of the Charter of Fundamental Rights of the European Union recognises the universal right to privacy. The European Court of Justice (ECJ), the European Data Protection Supervisor (EDPS) and the European Fundamental Rights Agency (FRA) oversee the implementation of those laws. In recent years, both the ECJ and the EDPS have been very active in the field of data protection: in 2014, the Court ruled that the retention of telecoms data violated fundamental rights. It has also ruled that search engines (such as Google) must remove links with personal information that the EU deems to be inaccurate, inadequate, irrelevant or excessive (the so-called 'right to be forgotten'). More recently, the ECJ declared, in its ruling on the Schrems case (discussed later), that the US did not provide an 'adequate' level of protection for European data and declared that an existing US-EU agreement on data transfers (the 'Safe Harbour' agreement) was invalid.

While data protection has been a core area of the European Union's law-making process, the US has adopted a patchwork approach, combining state legislation, guidelines and self-regulation. But this does not mean that US citizens do not have privacy rights. The Fourth Amendment to the Constitution ensures that US citizens enjoy "the right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". The Supreme Court has recently confirmed these rights in the landmark cases United States v. Jones and Riley v. California. But the US has struggled with understanding the spirit of the Fourth Amendment in the digital age – several draft laws have foundered because no one could agree exactly what it was legitimate to look at and what was not. These struggles explain why there is no comprehensive federal data protection law other than the outdated 1974 Privacy Act. This regulates the processing of personal data in the US but it provides for numerous exceptions which in effect limit the privacy rights of individuals. Although there are some federal laws (such as the Health Insurance Portability and Accountability Act), that regulate data privacy, they only do so in specific areas. Many US states do not have data protection laws, either. There are no US equivalents to the European Data Protection Supervisor, or even to the national data protection authorities. But both the Federal Trade Commission and the Privacy and Civil Liberties Oversight Board have some responsibilities for overseeing privacy rights.

The US and the EU also approach consumer privacy in different ways: the US has been much less keen to regulate the ability of companies to move data around and share it with other companies – and the public. But both deal with citizens' privacy in a similar fashion: governments on each side of the Atlantic allow their respective intelligence agencies some rights, in certain circumstances, to breach the privacy of citizens and residents.[11] Countries including Germany, France and the UK have extensive surveillance systems in place (such as TEMPORA in the UK and 'Frenchelon', in France).[12] Despite European outrage at revelations of US surveillance activity in Europe, in some respects, Europe is much closer to the US than a lot of people care to admit.

8: Kristin Archick, 'US co-operation against terrorism', Congressional Research Service, December 2014.

9: Mary Madden and Lee Rainie, 'Americans' attitudes about privacy, security and surveillance', Pew Research Center, May 20th 2015.

10: Michael Friedewald, Marc van Lieshout, Sven Rung, Merel Ooms and Jelmer Ypma, 'Privacy and security perceptions of European citizens: A test of the trade-off model', EU Privacy and Security Mirrors project (PRISM), IFIP International Federation for Information Processing, 2015.

11: David Cole and Federico Fabbrini, 'Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders', in Federico Fabbrini and Vicki Jackson (eds), Constitutionalism Across Borders in the Struggle Against Terrorism, Edward Elgar, 2015.

12: The existence of TEMPORA, a surveillance programme used by the British Government Communications Headquarters to trace internet communications, was revealed by Edward Snowden. 'Frenchelon' is reportedly a network of spying antennas operated by the French Directorate General for External Security (DGSE in French). Emails related to the operation of 'Frenchelon' were exposed by Wikileaks.

Friends, not foes: Restoring trust in EU/US data flows

In recent years, political attitudes to privacy and security have shifted in the US: the Obama administration, eager to distance itself from George W Bush's global 'war on terror', has been more open than its predecessor to a transatlantic dialogue on privacy and security. In an unprecedented move, US attorney general Eric Holder announced in June 2014 that the US would introduce legislation granting EU citizens judicial redress in America; this would mean that European citizens could ask American courts to examine cases where law enforcement's use of their data might have violated their privacy. Currently, the US only grants this right to American citizens. The judicial redress bill – not yet adopted – shows that the Obama administration understands that transatlantic negotiations on security cannot progress unless the US responds to European data privacy concerns.

After the Snowden revelations, Europe and America have been working hard to restore the trust that underpins transatlantic data flows. As a result, they are currently reviewing existing agreements and adopting new treaties. For example, the EU and the US have recently finalised negotiations on the 'data protection umbrella agreement'. This agreement seeks to establish a common, permanent framework to govern transatlantic data flows for the prevention, detention, investigation and prosecution of crime. Both sides hope that the agreement will reduce tensions when they negotiate, and implement, future ad-hoc agreements on data transfers for law enforcement purposes. The text of the data protection umbrella agreement has largely been agreed by EU and US officials, but will only come into force once the US government adopts the judicial redress bill.

Privacy and data protection are also among the public concerns raised by the US-EU Transatlantic Trade and Investment Partnership (TTIP). The European Parliament has asked the European Commission to exclude data protection and privacy from the TTIP negotiations. Currently, the EU requires that companies transmitting data to the US ensure that there is adequate protection of consumer data, essentially equivalent to that of the EU. The Parliament and privacy activists fear that TTIP provisions on data flows (including a potential chapter on e-commerce) could circumvent the application of EU data protection rules to US companies operating in Europe. Although the negotiations are (mainly) secret, the Commission has said that data protection standards will not be part of TTIP negotiations, and that "TTIP will make sure that the EU's data protection laws prevail over any commitments."[13]

Despite recent developments, the improvement of transatlantic relations in the field of data flows remains a work in progress. Tensions between the EU and the US persist, and extend to American companies operating in the EU. Many Europeans are concerned about the way US online service providers, such as Facebook or Google, use their data. This could endanger the business of these companies in Europe. The ECJ's recent ruling in Schrems, discussed below, is a case in point.

"In some respects, Europe is much closer to the US than a lot of people care to admit."

Sailing adrift? The impact of disagreements over privacy on transatlantic business

The EU Data Protection Directive, passed in 1995, prohibits the transfer of EU citizens' data to countries that do not ensure an adequate level of protection for it. In 2000, the European Commission recognised the 'Safe Harbour' privacy principles issued by the US Department of Commerce as adequate protection. As a result, US multinationals, such as Facebook, which certified that they adhered to these principles, were allowed to transfer data from EU countries to servers located in the US. But in November 2013 the European Commission asked the US authorities to review the Safe Harbour system and made 13 recommendations to make the scheme fully compliant with EU legislation. And in October 2015, the European Court of Justice struck down the EU-US Safe Harbour agreement.

This landmark ruling came after Maximilian Schrems, an Austrian law student, had taken Facebook to the ECJ. He argued that, in the wake of the Snowden revelations, the US could no longer be considered a country offering an adequate protection of personal data. The lawsuit specifically asked whether national data protection authorities in Europe were bound by the Commission's judgement that the US provided adequate data protection – even when there were strong suspicions that this was not the case. Advocate General Yves Bot released his controversial opinion on September 23rd, 2015. In it, Bot recommended that the ECJ allow national data protection authorities to examine claims of breaches under the Safe Harbour agreement. He also advised the ECJ to declare the agreement invalid, which the court duly did.

The ruling is a clear case of the ECJ overstretching its competences to "change the way the internet is governed as regards personal privacy."[14] The Schrems case dealt with a preliminary ruling that had been referred to the ECJ by the Irish High Court – where Facebook's European subsidiary is located. In its question, the Irish upper court did not ask the ECJ to decide on the validity of Safe Harbour. It only requested

13: Directorate General Trade, European Commission, 'Factsheets on TTIP', 2015.

14: Hugo Brady, 'Twelve things everyone should know about the European Court of Justice', Centre for European Reform, July 2014.

that it determine whether a national data protection authority could examine a potential breach of data protection rules under Safe Harbour. The EU judges not only allowed national data protection authorities that competence, but also turned to examine the compatibility of the Safe Harbour agreement with EU law. According to the Court, since national courts or data protection authorities could not, even if they wanted to, overturn a Commission decision, it was only logical that the ECJ (the only institution with competences to invalidate an EU act) would do so.

In the ECJ's view, the US does not offer an adequate level of protection to European data. The ECJ considers that, to pass the 'adequacy' test, countries should have privacy rules which are similar to those of the EU. This has the effect of extending the territorial application of EU rules worldwide. To justify its finding that the US does not offer sufficient protection to European data, the ECJ alluded to the revelations made by Edward Snowden. Neither the US government nor Facebook were part of the proceedings, not even as *amicus curia* ('friends of the court') who may present evidence while not being part of the formal proceedings. The Court made its finding purely on the basis of press reports and third party allegations. The supreme court of the EU should avoid such behaviour, which has justifiably sparked ire in the US.

The ECJ ruling entails several bad consequences for Europe. It creates regulatory uncertainty for those 4,500 companies that rely on transatlantic data flows for some or all of their activities, including IT and internet firms, but also banks, retailers and manufacturers.

The regulatory burden arising from the ruling will be more easily borne by large digital incumbents, which are mostly American, precisely at a time when the Commission hopes to give a boost to European digital start-ups.[15] After the ruling, the Commission issued guidelines explaining how companies can continue to legally send data to the US. But the guidelines give few details.

In the meantime, businesses have to rely on cumbersome ways to work around the problem. These include 'model contracts', clauses agreed with EU authorities on data transfers between EU and non-EU companies, or individuals. But these contracts could also be open to legal challenges. Then there are 'binding corporate rules' – bespoke agreements adopted by corporations, which govern data transfers between a company's operations in different countries and which require EU approval. These rules are costly to draft and the EU must agree them with every company separately. The most wasteful, but possibly more legally robust solution, is for companies to hold data storage centres in Europe to exclusively hold EU citizens' data, rather than transferring it to the US. In November, Microsoft unveiled plans to set up such a centre in Germany. Only large companies can afford this approach.

The ruling may also erect barriers to data flows within the EU. The ECJ has allowed all 28 national data protection authorities to review the adequacy of privacy standards in countries outside the EU. National data watchdogs may interpret these non-EU standards differently, leading to a situation where data could be transferred legally to America from one member-state but not from another. Such uncertainty and fragmentation is not only bad for the single market – but also for EU citizens, who may see their privacy rights better protected in some national jurisdictions than in others.

"The Schrems ruling imposes a regulatory burden which large digital incumbents (mostly American) will bear more easily."

The Court's decision could contribute to the fragmentation of the internet. One of the internet's main benefits for citizens and companies is the free flow of information across the globe. An open internet is in Europe's interest. However, China, Russia and other authoritarian countries are seeking more national control over it. The EU has been co-operating with the US and others at multilateral forums, like the Freedom Online Coalition, to keep the internet open. But Europe's credibility is now tarnished, as the ECJ has questioned the exchange of data between two of the staunchest proponents of a global internet.

The European Commission had started negotiations on a new Safe Harbour agreement well before the ECJ delivered its ruling on the Schrems case.[16] However, the new agreement could be delayed beyond January 2016, when a 'grace period' accorded by the Commission to US companies expires. The Commission has said it will not investigate breaches of privacy laws until then, but if negotiations drag on, US companies could become liable to penalties. The Schrems case will have an impact on the negotiations over a new agreement: the EU is demanding guarantees that the collection of European data for security purposes will be limited and proportional. But Washington is clearly disappointed with the ECJ ruling, and may be reluctant to make concessions to a defiant EU. The disagreement over transatlantic data flows may also undermine the continuing transatlantic trade talks: while TTIP is intended to reduce transatlantic trade barriers, the

15: John Springford, 'Offline? How Europe can catch up with US technology', Centre for European Reform, July 2015.

16: The EU's data protection reform will also have an impact on the Safe Harbour system: the new regulation is likely to give the Commission the power to monitor, review, and revoke decisions on the adequacy of a country to receive data from European citizens.

ECJ is raising them. European officials have hinted that TTIP might cover data protection – negotiations are underway on e-commerce and other sectors that require transatlantic data flows – but the Schrems ruling means that a solution is more urgently needed than the TTIP timetable allows. Possibly, the recently concluded trans-Pacific trade deal, TPP, will allow US digital firms to expand more easily in Asian markets than in Europe. In Asia, US data standards are likely to be more readily accepted, while Europe's cumbersome data protection landscape may inhibit the roll-out of new services. The ECJ's decision in Schrems could also make the adoption of the judicial redress bill more difficult, if the US Congress reacts negatively to the EU's belligerence.

Encryption is another area where transatlantic disagreements affect American businesses in Europe. If a government wants access to encrypted data, it needs either to request an 'encryption key' from the online service provider – what the industry calls 'using the front door'– or use covert means to gain unlimited and unscrutinised access to the data, 'going through the back door'. The front door procedure is fairly straightforward when the government has jurisdiction over the online service provider: because the majority of big technology companies are based in America, the process of requesting information for law enforcement purposes is easier for the US government than for European countries. The latter need to request information through so-called Mutual Legal Assistance Treaties (MLATs), by which states agree bilaterally or multilaterally to co-operate in criminal cases. The EU and the US signed an MLAT in 2003, before the EU was given competence in justice and home affairs under the Lisbon treaty. The EU-US MLAT applies in cases where the member-state concerned does not have a bilateral MLAT with the US.

The MLAT procedures are cumbersome and lengthy. For example, requests from the US to the UK can take up to 13 months, and the procedure is even more complicated in cases where the countries do not share a common language, because requests must then be translated.[17] Not only are MLAT requests slow, but they are frequently denied due to confusion over data protection rules.[18] The Council of Europe says that the MLAT process is inefficient, especially when agencies are trying to get electronic evidence.[19]

The inefficiency of MLATs is not only a problem for European governments; it also makes it difficult for the US to access European data for law enforcement purposes. In 2013, the US Department of Justice (DoJ) issued Microsoft with a direct search and seizure warrant, to obtain data from an Outlook account located in Ireland. The DoJ decided to issue a warrant, instead of asking the Irish authorities to retrieve the information through an MLAT procedure, because the latter took too long. The US government argued that, in the time it took for the request to be processed, the information could be moved out of the account. Microsoft has challenged the warrant, because if the company complied with it, it would mean that the US Department of Justice would have jurisdiction over foreign states.[20] This would put US companies in a tricky position in which they would be obliged to comply with contradictory laws and requests. Microsoft argues that such a result could "force American companies to entirely pull out of certain markets".[21]

"Banning encryption would be bad for citizens' privacy and erode consumers' trust in US tech companies."

It is time to reform the MLAT system: over time, it has proved to be inefficient, opaque and expensive. What is more, when using the front door becomes too complicated for EU governments, they are likely to seek access through the back door by, for example, banning encryption. This would be detrimental to citizens' privacy and erode the already weakened trust that consumers have in US tech companies.

If the EU and the US do not alleviate these tensions, transatlantic trade could suffer. According to a 2014 Brookings Institution study, data flows between the US and the EU are the highest in the world. Data transfers are a form of international trade. And they have a significant value for Europe's economy: in 2012, EU exports of digitally deliverable services (such as software or royalties) to the US were worth $86.3 billion.[22] European politicians sometimes seem to be more concerned with creating a European Google or Facebook, than with the data protection rules which would allow Google and Facebook to operate in the EU without compromising Europeans' desire for data privacy. Digital companies, such as online service providers, need a predictable legal environment that treats them equally, regardless of their nationality. They also depend on their customers' trust. Cases such as Schrems, or Microsoft Ireland, threaten to drive American tech companies out of the European market. This is neither in Europe's nor in America's interest.

17: Gail Kent, 'The Mutual Legal Assistance problem explained', Centre for Internet and Society, Stanford Law School, February 23rd 2015.
18: Jonah Force Hill , 'Problematic alternatives: MLAT reform for the digital age', Harvard Law School National Security Journal, January 28th 2015.
19: T-CY Cloud Evidence Group, 'Criminal justice access to data in the cloud: challenges', Council of Europe, May 26th 2015.
20: Sergio Carrera, Gloria Gonzalez Fuster, Elspeth Guild and Valsamis Mitsilegas, 'Access to electronic data by third-country law enforcement authorities: challenges to EU rule of law and fundamental rights', Centre for European Policy Studies, July 8th 2015.
21: Jonah Force Hill , 'Problematic alternatives: MLAT reform for the digital age', Harvard Law School National Security Journal, January 28th 2015.
22: Joshua Meltzer, 'The importance of the Internet and transatlantic data flows for US and EU trade and investment', Brookings, October 2014.

Fixing the EU's privacy and security problem: A set of recommendations

Europe's privacy and security problems are serious, but not terminal. Policy-makers need a new approach that will close security gaps while protecting citizens' rights. Here are some ideas that may help them to do so.

Talk to them: Giving the European Parliament access to confidential information

At present, only those MEPs who have security clearances from their governments can gain access to confidential information at the EU level. There is no uniform EU clearance procedure and there are no plans for one. The EU does not have a body that can carry out vetting, procedures for which differ greatly from country to country, so some MEPs find it easier than others to obtain clearances. Many MEPs are not prepared to go through the stringent process of getting security vetted. In some countries, this includes exhaustive checks and interviews with direct and distant family members. As a result, only a handful of MEPs are currently security cleared.

For its part, the Council has set up a secure room in the Justus Lipsius building (its headquarters in Brussels) for the few MEPs who are security-vetted to review sensitive intelligence material. This room is under surveillance to ensure that there are no leaks that might compromise member-states' security. Visitors are requested to leave their phones and other electronic devices outside. But Council officials claim that it is difficult to convince those parliamentarians who are security-cleared to make use of the room.

Consequently, MEPs feel under-informed, the Council gets frustrated and nothing gets done. These problems could be solved if the EU decided to put a formal structure in place, so that when new security measures are under discussion the Parliament has to review relevant confidential information and the Council must disclose this information.

The parliamentary review could be carried out by a sub-committee within the Parliament's LIBE committee, mirroring the US Congress' Committee on Homeland Security. A similar sub-committee exists within the EP committee responsible for foreign affairs (AFET), by virtue of an inter-institutional agreement between the Parliament and the Council. The remit of this sub-committee is restricted to issues related to the EU's Common Foreign and Security Policy (CFSP). So there is a regulatory framework in place to set up an equivalent justice and home affairs sub-committee. In fact, the LIBE secretariat has begun to examine the possibility of requesting that some LIBE members undergo security vetting.

23: This is currently the European People's Party (centre right); the Progressive Alliance of Socialists and Democrats (centre left); the European Conservatives and Reformists (the group including the British Conservatives); the Alliance of Liberals and Democrats for Europe (centrist); The European United Left/ Nordic Green Left; and the Greens/European Free Alliance.

This sub-committee would be charged with examining the necessary intelligence material to enable the Parliament to take a fully informed decision on the security measure under discussion. For example, national security services could brief the members of this sub-committee on plots that have been foiled thanks to the tracing of air travellers' data. MEPs should be allowed to request information, but national security services should also be allowed to refuse these requests, for non-trivial reasons. For the system to work, a 'chain of trust' would need to be built between the sub-committee, the LIBE committee and the plenary, in which all MEPs debate and vote on laws. The proposed security sub-committee would take decisions based on the information provided by the Council, and make a recommendation to the LIBE committee. But the members of the sub-committee would commit not to reveal sensitive material to any other MEP. LIBE would need to trust the advice of the selected MEPs, and the plenary would, in turn, need to trust LIBE.

"A security sub-committee could examine intelligence material so that the Parliament can take fully informed decisions."

Political groups in the European Parliament could nominate their representatives to this sub-committee. For political reasons, the Parliament would probably need to set a minimum number of MEPs for a political group to gain representation in this sensitive body. Setting such a threshold would be in line with practices at the national level: the Dutch parliamentary committee responsible for intelligence has such a limit. Political groups wishing to take part in this EP sub-committee could be required to have, say, at least 50 MEPs. This would mean that the sub-committee could be composed of 6 MEPs, one for each European political party that has 50 or more representatives in the Parliament.[23] Such a threshold would normally prevent sensitive information being passed to extremist or racist parliamentarians – and it would have the added benefit that the sub-committee would have a stable, long-term membership, as bigger groups are less likely to collapse.

All members of this sub-committee should have security clearance. This may require a 'gentleman's agreement' by the Council to ensure that member-states facilitate the clearance of MEPs on the sub-committee. The Council does not have the competences to issue security

clearances; only national governments do. But the Council could encourage national administrations to vet parliamentarians who are part of the sub-committee, especially in cases where clearances are more difficult to obtain. There is a very good example of how this could work: when launching a competition case against a company, the European Commission allows lawyers for the parties to examine relevant documentation in a secure room at DG Competition. Attorneys are allowed to use that information to build their case, but are forbidden to discuss it with their clients in order to protect sensitive commercial information. A 'chain of trust' is established between the Commission, which trusts the lawyer not to reveal sensitive information; the lawyer, who commits to use the information only for the purpose of defending his or her client; and the client, who has to trust the lawyer without having full access to the Commission's information.

A security sub-committee in the Parliament would help to overcome some of the misunderstandings between the Parliament and other institutions. But the system will not work if the Council and the Commission do not engage in a more open and honest dialogue with the European Parliament. This, in turn, would be easier if the Commission and Council did not sometimes over-classify documents. The EU has five levels of document security. They are (from more to less sensitive): 'Top secret'; 'Secret'; 'Confidential'; 'Restricted'; and 'Limited'. Access to anything from 'Confidential' upwards requires a security clearance. But the process for classifying documents in the EU is unclear: there have been instances where the same document has been given two different levels of security, and others where documents have been classified merely because they made an EU department look bad.[24] What is more, it is difficult for parliamentarians to declassify documents. MEPs are discouraged from requesting the declassification of a document, or access to a document which they suspect has been over-classified. The Council and the Commission should ensure that the classification procedure responds to legitimate security needs.

Building bridges: Improving transatlantic relationships and protecting citizens on both sides of the Atlantic

Reform the legal framework for transatlantic data transfers

A new Safe Harbour agreement will not do much to improve transatlantic relations. The Schrems case shows that a system where companies self-certify their compliance with EU law, subject to periodic review by the European Commission, is undesirable, because it creates legal uncertainty. It would be better to agree on common EU-US standards on what companies can and cannot do in relation to consumer privacy, and create a single transatlantic market for data.

The new general data protection regulation proposed by the Commission tries to address this issue. It allows companies to adopt binding corporate rules or standard contractual clauses if they wish to transfer data to a third country.[25] But these would still be private schemes that could result in different data protection rules for different companies. A bilateral agreement with broad standards between the EU and the US would offer more stability than extending binding corporate rules, which would in essence be a self-regulation scheme. The draft proposal for a data protection regulation foresees that the EU can conclude international agreements on transfers of data to third countries. A transatlantic treaty could outline the data protection principles to which companies wishing to carry out transatlantic data exchanges would need to adhere.

"A new Safe Harbour will not improve transatlantic relations. It is better to agree on common EU-US standards."

The transition from a self-regulatory scheme to a legally binding one will not be easy and will probably take some time – especially as a treaty will need to be approved by the European Parliament. But there are reasons for optimism: the data protection umbrella agreement, which regulates the transmission of data for law enforcement purposes, shows that the US and the EU can find common ground for protecting transatlantic data flows. They should explore the possibility of finding such understandings for areas other than law enforcement. Moreover, the US proposed bill on judicial redress and the revision of the 'Safe Harbour' principles show that there is the political will to move transatlantic negotiations on privacy and security forward.

Address the question of mass surveillance

The revision of the 'Safe Harbour' principles (or even a forward-looking bilateral agreement on commercial data transfers) would not affect states' ability to conduct surveillance. EU legislation governing the transfer of data for commercial and law enforcement purposes specifically excludes cases where data are collected for intelligence purposes. If the EU wants to fully address the question of mass surveillance, it would need to negotiate an additional agreement with the US. This could take the form of a reciprocal transatlantic framework to protect both US and EU citizens from unwarranted surveillance, as suggested by two law professors, David Cole and Federico Fabbrini.[26] Such

24: Andrew Rettman, 'What is Secret UE anyway?', *EU Observer*, September 24th 2012.

25: The current data protection directive only marginally mentions contractual clauses.

26: David Cole and Federico Fabbrini, 'Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders', in Federico Fabbrini and Vicki Jackson (eds), Constitutionalism Across Borders in the Struggle Against Terrorism, Edward Elgar, 2015.

an agreement would extend the constitutional protections enjoyed by nationals in the context of surveillance activities, to foreign citizens, which would reinforce privacy rights on both sides of the Atlantic. It would, likewise, help to restore trust in transatlantic co-operation on security issues.

Strengthen Europol's role in intelligence matters
Co-operation between the EU and other international partners would be easier if Europol acted as a conduit for information between EU member-states and third countries, such as the US. Transforming Europol into some sort of 'European FBI' is out of the question. But recent developments show that Europol could (and should) play a bigger role in transatlantic intelligence co-operation.

The US recently posted security attachés to Europol to try to promote it as a single point of contact. When the Parliament asked for an EU institution to supervise American data requests under the TFTP agreement, the US argued that it should be Europol. The Commission's European Agenda on Security, released three months after the *Charlie Hebdo* attack, also advocates a bigger role for Europol in the field of intelligence, counter-terrorism and data transfers, including the establishment of a European counter-terrorism centre (which will begin operations in January 2016). After November's terrorist attack in Paris, the EU justice ministers agreed to make better use of Europol for intelligence-sharing purposes. The EU is in the process of revising the regulation that governs the functioning of Europol, and could use this opportunity to clarify and enhance the role of the agency as the first point of contact for intelligence exchanges and co-operation with international partners. This will not be easy: some of the biggest member-states prefer their well-established bilateral agreements.

Europe as a whole would benefit from having a more centralised approach to information-sharing, as the November attacks in Paris have shown. The Union's police body is the best placed institution to receive vital information such as the US no-fly list (which it does not yet share with the EU) – not only because the US trusts it to handle confidential information, but also because it could ensure that the list is communicated to all member-states, through the right channels. Europol could help to prevent future terrorist strikes: the *Charlie Hebdo* attack might have been foiled if the French police had known that the Kouachi brothers were suspected by the Americans of having terrorist connections; and French authorities might have known more about Belgian citizen Abaaoud's plans had they received more information from other countries.

Reinforce privacy rights by reforming encryption rules

Encryption is a very powerful tool to protect the privacy of citizens and consumers alike. The monitoring of communications and patterns of online behaviour helps to disrupt criminal activities. But European governments should not try to become omniscient 'Big Brothers'. In most countries, only a judge can allow the recording of conversations in people's private spaces, after police have established that the suspect is likely to have committed a crime. For a democratic state, the digital world should be no different. Governments should accept that even citizens with nothing to hide may want to protect their personal data from prying eyes on the internet (whether governments or hackers), and that it is reasonable for individuals to use a certain level of encryption to that end.

> *"Governments should accept that even citizens with nothing to hide may want to protect their personal data."*

Of course, law enforcement should still be able to access information and data when necessary, particularly in urgent cases. Ideally, they should do that by going through the front door – with the exception of emergencies, such as that which followed the November 2015 Paris attacks. Under state of emergency laws, the French government, for example, is allowed to suspend certain constitutional rights, such as communications privacy and freedom of assembly. This applies both in the digital and physical worlds. But in ordinary times, law enforcement bodies need to use legal channels that allow citizens to understand, and challenge, governments' use of their data, in cases when they are prosecuted. Currently, using this front door (requesting information from non-European companies through Mutual Legal Assistance Treaties) is complicated for European governments. The rules governing MLATs were drafted before the internet took off, and as a consequence do not address core issues such as what to do when a subsidiary company holds data overseas – the main issue in the Schrems case.

Some governments want to ban encryption. The Netherlands and France are already drafting and implementing laws to this effect. This is not only detrimental to citizens' rights, but also to the operation of technology companies in Europe.

On encryption, European governments should follow the advice of David Anderson, the UK's independent reviewer of counter-terrorism legislation. In his 2015 report, he regretted that some governments were still asking to "insert back doors into any telecommunications" and he advocated "a law-based system in which encryption keys are handed over (by service providers or by the users themselves) only after properly authorised requests".[27] The German

27: David Anderson, 'A question of trust: Report of the investigatory powers review', June 2015.

government also believes that encryption helps to ensure internet safety.[28]

Of course, encryption helps terrorists to hide their activities from security services. But so does talking in the street rather than on the phone. In fighting terrorism, EU governments should not play in the hands of criminals and suspend civil liberties all together. With the appropriate mechanisms in place (speedy judicial authorisation to break encryption, and a close co-operation with online services providers, for example), security services can trace suspects without compromising the fundamental rights of EU citizens.

The European Commission is currently reviewing the EU-US MLAT, and reform is needed. One of the primary causes of the bottlenecks in handling MLAT requests is lack of resources; governments should spend more on processing them. They should also review their procedure for eliminating duplication: currently, several agencies are involved in processing MLAT requests and their actions sometimes overlap. For example, there are six authorities involved in US-UK MLAT requests, including a 'central authority' in each country, which is ultimately responsible for verifying the requests. Finally, governments should establish a secure, standardised web-based mechanism to send requests. At the moment, requests need to be sent either by normal e-mail or by post, which makes processing them more time-consuming. The US President's Review Group on Intelligence and Communications Technologies has recently underlined that an online submission form and clearer information about MLAT requirements would improve the system.[29]

Conclusion

The threat to Europe's security is real. Terrorism and organised crime have become increasingly transnational, and the EU is in many respects better placed than member-states to implement measures against cross-border crime. But these measures often interfere with citizens' civil liberties, not least their right to privacy. The European Parliament has been blocking essential legislation in this area, and many Europeans have lost trust in the US despite the urgent need for transatlantic co-operation in combating terrorism.

If the EU does not find a way out of these problems, the security of 500 million Europeans could be compromised. With Europe's patchy approach to counter-terrorism measures, terrorists may exploit legal loopholes. America may decide to bypass the EU and conclude bilateral agreements with the member-states – agreements that would worsen an already fragmented approach to security. As a result of this fragmentation, American technology companies will face an increasingly complicated business environment. Such a lack of regulatory consistency will damage Europe's economy as well as America's.

The EU needs to reconcile its competing interests on privacy and security. It therefore needs to improve communication between the European Parliament and the Council, strengthen its relationship with the US and promote the development of technologies that offer 'privacy by design', such as encryption.

These reforms will not be easy. But they are necessary to ensure that Europe can remain a safe place, impose fewer costs on companies and champion civil liberties.

Camino Mortera-Martinez
Research fellow and Brussels representative, CER.

December 2015

This publication is supported by the Open Society Foundations.

28: Federal Government of Germany, 'Germany's Digital Agenda, 2014-2017', 2014.

29: The White House, 'Liberty and security in a changing world', December 12th 2013.