

The End of the Road for Personal Data Protection in the EU

JURIST Guest Columnist Virginia Keyder, currently teaching European Union law at Bogazici University and Sabanci University in Istanbul, Turkey, says that while the European Commission, aided most recently by the Advocate General of the European Court of Justice, has taken steps to encourage and even mandate increased state data retention for more efficient crime-fighting in the EU, the trend threatens to limit fundamental individual rights in the name of an ever-widening definition of "state security"...



The European media has recently been awash with horror stories of government excess in the area of electronic surveillance and retention (and loss) of personal data. On November 5, Robert Verkaik of UK newspaper The Independent discussed the public outrage that greeted the government announcement of "plans to create a database holding information about every phone call, email and internet visit made in the UK". And yet, the European Commission, aided most recently by the Advocate General of the European Court of Justice (ECJ), has set its sights on not only assisting such excesses, but mandating them.

For readers unfamiliar with the structure of the European Community, the European Union and the relationship between the two, this may be hard going. I ask you to bear with me because involved in this ostensible struggle for increased legislative competence is a concerted effort to limit fundamental individual rights in the name of 'state security' in an ever-widening sense.

On October 14, 2008 ECJ Advocate General Bot upheld the competence of the EC Council (the body that votes on legislation in the European Community) to enact Directive 2006/24EC (On the retention of data generated or processed in connection with the provision of publicly available electronic communications network and amending Directive 2002/8) based solely on the single market competence afforded by the EC Treaty. AG Bot rejected a claim by Ireland that such legislation should have been enacted under EU's 'third pillar', i.e. Judicial and Police Cooperation, and found instead that single market competence under Article 95 of the European Community Treaty (TEC) was sufficient.

Article 95 TEC gives the EC the power to "adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."

The purpose of Directive 2006/24 is set out in its Article 1(1):

This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications

networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

Article 5 of the Directive sets out the data to be retained. The categories are as follows (the details are set out under each category):

- a. data necessary to trace and identify the source of communication;
- b. data necessary to identify the destination of the communication
- c. data necessary to identify date, time and duration of the communication;
- d. data necessary to identify the type of communication;
- e. data necessary to identify users communication equipment or what purports to be their equipment; and
- f. data necessary to identify location of mobile communication equipment.

Article 8 provides that "Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay."

To the untrained eye, it would be hard to imagine a more straightforward attempt to legislate for the purpose of collecting and retaining data for the purpose of police cooperation among member states, an activity that falls squarely within third pillar competence.

The difference in legal competence underpinning European legislation, i.e. whether the EC does it or the EU does it, is important. At the risk of oversimplification, the difference between EU (third pillar) and EC (first pillar) competence stems from the creation of the European Union as a 'parallel institution' by the member states of the European Community in the 1992 Maastricht Treaty. Through the EU, EC member states could agree to measures and common positions in areas for which they desired to retain more national sovereignty than they could through the EC. The 'third pillar' of the EU (Judicial and Police Cooperation, or 'Justice and Home Affairs' between 1992 and 1999) sets out those areas where member states, acknowledging the need for common action, were nevertheless reluctant to give over full sovereignty, as they had in 1957. For example, the member states agreed to surrender considerable sovereignty to the EC for the establishment of free movement of goods, services, capital and labor, but not for judicial and police cooperation, for which they created the 'third pillar'. (For those curious but uninformed readers, the missing second pillar is Common Foreign and Security Policy).

An act under the third pillar cannot affect the 'acquis communautaire' i.e. that body of Community law binding all member states, which includes treaties, secondary legislation and

ECJ case law. Third pillar actions cannot amend EC directives and retains 'intergovernmental' status, roughly comparable to a standard agreement under international law between totally sovereign states. It is not subject to important structural principles of Community law such as supremacy (of EC law) and direct effect (on individuals). It is also significant that EU legislation (i.e. acts under the third pillar) requires unanimity making it more difficult to conclude, while TEC Article 95-based legislation may be passed by a qualified majority of votes in Council.

The reasoning behind the AG's opinion favoring EC single-market legislative competence is puzzling. The opinion twists and turns through exemptions and retained national competences of earlier EC directives on the subject of data protection that Directive 2006/24 is designed to amend, and then, after acknowledging the stated crime-fighting purpose of the legislation, the AG supports his decision to view Directive 2006/24 as single market legislation as follows (paragraph 85):

In the absence of harmonisation, a provider of electronic communications services would be faced with costs related to the retention of data which differ according to the Member State in which he wishes to provide those services. Such differences may constitute obstacles to the free movement of electronic communications services between the Member States and may therefore create obstacles to the establishment and functioning of the internal market in electronic communications. They may, in particular, slow down the cross-border development of new electronic communications services which are regularly introduced in the information society. They may also give rise to distortions in competition between undertakings operating on the electronic communications market.

Totally absent from the opinion is any mention of the importance with which the protection of personal data has been viewed by member states over the past three decades and within the legal structure of the European Community since 1995. This positivist approach to what constitutes a pivotal area of fundamental rights is in sharp contrast to the privileged position Europe has given to a growing body of human rights law over the past half century.

The Background of Personal Data Protection

Personal data protection in Europe is an important offshoot of the fundamental right of privacy as set out in the Council of Europe European Convention on Human Rights (ECHR) (Art. 8), the International Covenant on Civil and Political Rights (Art. 17) and the EU Charter of Fundamental Rights (CFR) (Art. 8). It has deep roots in post-WWII constitutions and legislation of EU member states, particularly Germany and France - two countries that have contributed heavily to the structure and substance of EC/EU law. As a human right, it is important to remember that privacy, along with other human rights, is a right that protects individuals from the State. The concept of 'privacy', as an instinct that drives us to walk off into a corner to talk on our cell phones or close the curtains when we are having sex has diluted the idea of privacy as a human right and made most of us associate it with our neighbors rather than the state. To understand the threat of having personal data lose the protection of the law requires that

privacy be repositioned as a fundamental human right against actions by the state.

Concern for personal data protection was initially the result of a long-standing belief in Germany, where such protection began, that the facility with which pre-war abuses of human rights and personal dignity were carried out, was at least partly attributable to the excessive accumulation of personal data by the Nazi regime (made possible a purpose-built census designed for the regime by IBM in 1933). In the 1990s, the rapid growth of the internet, with its potential for instantaneous and universal dissemination of data, advanced telecommunications, and the new genetic and biometric technologies accentuated the need to protect the fundamental right of privacy in general, and the right to the protection of personal data in particular.

In 1995, the European Community undertook to protect personal data by enacting Directive 95/46. This Directive harmonizes the protection and free movement of personal data between member states in the context of the single market. It sets common standards of data protection so as to prevent national law from prohibiting the free movement of data among member states. It includes the proviso that personal data should not be sent to any non-member state unless it is established that the recipient state provides a similar level of legal protection to personal data.

Two years later, Directive 95/46 was joined by Directive 97/77 (on data protection in the telecommunications sector) and by Regulation 2001/45 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies (as distinct from the member states) and on the free movement of such data was enacted. This Regulation established a monitoring body, the European Data Protection Supervisor (EDPS), and sanctions for offenders. Like the two directives, it applies not only to data movement within the EU but to personal data sent to non-member states. Article 9 requires that 'personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46, if an adequate level of protection is ensured in the country of the recipient...".

Article 3(2) of Directive 95/46 states that "This Directive shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense, State security (including economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."

What we see in this article is a line being drawn between EC competence, i.e. that which the EC can rely on to enact legislation in connection with harmonization for purposes of constructing a single market, and EU competence, in areas of public security, defense, etc.,

and member state criminal law competence. Titles V and VI of the TEU are the second and third pillars, respectively. The inclusion of economic well-being of the state is interesting but deserves further attention than the scope of this essay offers.

Under these two Directives, the collection of and access to personal data is limited in use and duration to legitimate purposes for reasonable periods of time. Holders of such data are prohibited from sending it outside the EU to any country which does not have similar data protection laws. Following the enactment and implementation of the Directives in the member states, strict limitations were therefore placed on data collection and retention as well as on transfer of personal data to non-member states.

Globalization, 9/11 and the Decline of Personal Data Protection

Europe does not live in a vacuum, however, and events subsequent to 1995 were soon to test the strength of personal data protection in the EC. The unfolding in the 1990s of 'globalization' with its expanding communications technology and its facilitation of transnational crime and then the events of September 11, 2001, introduced serious threats to many individual rights once believed to be central to the self-image of western countries, among them the protection of privacy. The US 'war on terror' and overriding claims of 'national security', especially in their international manifestations, combined with heightened interest in preventing and prosecuting criminal activity ranging from drug and human trafficking to economic crimes such as intellectual property offences. This exacerbated the fundamental tension between state (and economic) interests and individual privacy in Europe as well as in the US (as seen in the wiretapping escapades of the National Security Agency).

In November 2001 the US enacted legislation requiring all air carriers to provide the US customs authorities with access to extensive electronic data on all passengers entering or leaving the US (passenger name records, or PNR). Such data once obtained could effectively be retained and circulated for the lifetime of the data subjects. Initially, the EC Commission advised the US that transferring such data would conflict with EC and member state data protection laws, particularly since the US has no data protection laws, let alone laws on the level mandated by Directives 95/46 and 97/77. US pressure on Brussels, combined with the threat to fine all airlines \$6000 per passenger entering the US without the requested data, led the EC Commission to issue a Decision to the effect that they were satisfied that the data protection required by Directive 95/46 existed in the US. This was designed to open the way to an agreement whereby data on all passengers entering the US would be provided by the airlines. No provision for extracting data on US passengers entering Europe was requested, and none was given.

Again, it is important to note that the US effectively has no data protection legislation (the first US state to enact such legislation was California, in 2003). Nor does it claim to have such

protection. Quite the opposite: data is seen as a valuable commodity which is readily transferred, bought and sold in the 'free market'. Individuals' rights regarding the data held on them is effectively limited to finding out what data is held, and potentially correcting it where it is found to be in error. This right is limited to US citizens. The US made no claims that the data would not be distributed among relevant agencies, and stored by private companies under the all-pervasive 'privatization' policies of the current US government. Opposition to this arrangement was widespread among data protection activists in Europe, however, and no formal agreement was signed at that time.

By early March 2004, however, noting "The fight against terrorism, which justifies the proposed measures" to be "a key priority in the European Union" and seeking to alleviate the "uncertainty of air carriers and passengers and their financial interests" in the absence of a concrete agreement, the Commission issued a Decision to enter into an agreement under which airlines would be authorized to provide the personal data requested by the United States. The European Parliament almost immediately requested a new Decision that would guarantee passengers the fundamental right of protection of their personal data. Failing to obtain such a Decision, the Parliament along with the EDPS brought an action before the European Court of Justice (ECJ) against the Council (the EC institution that votes on all legislation) to annul the Decision on the basis that the EC had no competence to enter such an agreement, that it breached the fundamental principles of the Directive on data protection, and that it violated fundamental rights of individuals as well as the EC principle of proportionality (a basic principle of EC law which restricts acts of the Community to what is necessary and proportional to the legitimate goal to be achieved in a democratic society).

To make a long story short, the ECJ set aside the decision on adequacy of US data protection on the basis that the goal of collecting the data, i.e. security and criminal law, fell outside the data protection Directive's purview, as stated in the Directive itself and set out above. Thus, said the Court, the need to evaluate whether the comparable protection required in the directive exists in the US never arises. The Court also found that the EC Treaty did not in fact provide an adequate legal basis for the Commission to enter into an agreement with the US to transmit personal data. The ECJ therefore found no need to decide whether or not fundamental rights would be violated by the Agreement. The so-called Agreement was a dead letter.

The EU remained under pressure from the US, however, and proceeded to assure the US that it would comply with its requests. In its capacity as the "EU" (or, lack of capacity, since the EU, unlike the EC, has no legal personality to enter into an agreement, though this didn't seem to bother anyone) it entered into an agreement to provide the data, such agreement to be given legislative effect by an EU Framework Decision assuring the compliance of all EU member states. The Agreement was signed on 23 July 2007. A week later, (according to EU doc. No. 12307/07, linked to Statewatch website) the US Dept. of Homeland Security requested that all negotiation documents related to the PNR Agreement be kept secret for ten years.

As the deadline for European compliance with US demands approached in 2007, and perhaps worrying the European population might be bothered by giving up so much (data and protection) and receiving so little (for throughout the negotiations it apparently never occurred to the EC or the EU to ask for reciprocal surrender of personal data of incoming passengers), the EU itself decided to institute its own PNR for passengers entering the EU. It began discussing plans to move beyond air traffic and impose such requirements not only on virtually all forms of travel into the EU, but even within the EU itself.

Although plans to extend the requirements to non-air travel have been put on hold, on November 11, 2007 the EU issued a proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes (COM 2007 (0654) final). Preempting claims that this violated fundamental rights, the opening sentence of the proposal states that 'Terrorism constitutes one of the greatest threats to... fundamental rights'. Noting that Directive 2004/82 already requires airlines to communicate Advance Passenger Information (API) to member states' authorities, it bemoans the fact that this is "sufficient only for identifying known terrorists and criminals". What it claims to need is a tool to carry out risk assessments of the persons, for obtaining intelligence and for making associations between known and unknown people." (Rumsfeld lives.) The proposal provides for retention of the data for 15 years and the only restrictions placed on transfer to third countries is that "(a) the authorities of the third country shall only use the data for the purpose of preventing and fighting terrorist offences and organized crime and (b) such third countries shall not transfer the data to another third country without express consent of the Member State (Proposed Article 8). Thus every member state would collect data on all passengers, and such data could be shared with third countries subject only to these restrictions. This is a far cry from the recognition, a mere 15 years ago, that entities, including states, collecting too much data have tended to abuse the data at the expense of individuals and fundamental rights. It is a far cry from Directive 95/46, which allocates competence to collect data for the purpose of state security, etc. to the full sovereignty of the member states.

The 2006 Directive

Meanwhile, back in the EC legislative theatre and pursuant to abovementioned rise in concerns about 'state security' and the 'war on terror', the EC passed Directive 2002/58 limiting the scope of the protection of personal data afforded in the original 1995 Directive. Article 15 of this 2002 Directive limited the right to data protection by enabling member states to restrict such rights "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". In essence, it allowed states to "adopt legislative measures providing for the retention of data for a limited

period justified on the grounds laid down in this paragraph". Notable here is the expansion of state powers from doing what is necessary to pursue terrorists to other unrelated acts including mere 'criminal offences' and unauthorized use of electronic communication systems.

There was little reaction to this 2002 Directive, however, and in 2006, Directive 2006/24 (the subject of the recent legislative competence decision by the AG) was enacted to amend the 2002 Directive by mandating data retention. Initially put forward by four countries to be adopted under EU third pillar competence (i.e. judicial and police cooperation, which as mentioned above requires unanimity and is not subject to the principles of EC law), it was seized upon by the Commission and passed as a Directive under the same competence as the earlier and now defunct agreement between the EC and the US, i.e. Article 95 for matters pertaining to single market.

It is this competence that was questioned by Ireland, and it is this competence that was accepted by the Advocate General in last week's decision.

Limiting Privacy in the State, the Community, and the Union

Anyone who follows the issues of privacy in Europe cannot help but notice that the decline in protection afforded the individual from the prying eyes of the state has been precipitous in recent years. Only Germany for example, among the 27 member states of the EU, found the introduction of 'body scanners' i.e. full exposure to border officials of passengers' naked bodies, to be an affront to human dignity (a concept itself enshrined in the German constitution). For the others, as for the US where the practice began, 'national security' seemed to justify the gross invasion of privacy of this 'strip search' technology. In its defense, it should be noted that European Parliament (the least powerful of all EC institutions) voted in October 2008 in favor of a Resolution alerting the EC to the potential for violation of both fundamental rights and the principle of proportionality (a general principle of Community law, similar to 'ultra vires' in the Common law, which restricts the powers of the EC to what is necessary and proportional in a democratic state to achieve its legitimate aims) entailed in such technology.

This decline the right to privacy is particularly marked in the UK where a database containing information on all individuals within the UK (this is separate from the communications database discussed in the opening paragraph of this essay), ranging from DNA and biometrics to data contained in various government databases, was recently proposed. The EU is itself about to embark on similar, if less invasive, projects. These include the Internal Market Information System, or IMI through proposed EC Directive 2008/49 (where the Commission relies on a previous decision of its own as a basis for legislative competence, much to the concern of European Data Protection Supervisor), and the EU Framework Decision on European Criminal Records Information System (ECRIS).

Government access to individuals' private records and documents has taken a great leap forward on both sides of the Atlantic. While personal data has never been subject to protection in the US, the recent US judicial recognition of the legality of the practice of allowing US border officials to take and copy hard disks of air passengers received little or no official comment in Europe. European companies fearing exposure of trade secrets, employee or contact information or other confidential data simply advise employees traveling to the US to go with empty computers and download documents necessary for their business upon arrival. Even this may not protect personal data and information contained on private hard disks, however, if last week's opinion by the Advocate General is upheld by the European Court of Justice and national measures like the UK 'blackbox' data base plans become law.

No Wonder Ireland Voted No

Last week's opinion by Advocate General Bot to the effect that EC Directive 2006/24, forcing member states to require Internet Service Providers to collect and save personal data of their customers, was properly passed by the EC under its treaty competence for building a single market will, if followed by the ECJ, provide just one more indication of a reversal of individual privacy rights built up over the past fifty years.

The fact that measures to limit data protection rights are now being taken at the European level, and thus subject to neither national constitutional nor electoral challenges, is doubly worrying. Such measures are unchallengeable once treaty competence to enact them is established. Ironically, the Charter on Fundamental rights with its Article 8 protection of personal data is inoperative until the Lisbon Treaty comes into effect. Rejecting Ireland's challenge to what seems on the face of it to be an obviously flawed legislative competence might not be the best way to gain support (from Ireland or any other member state given the opportunity to voice its opinion) for a Treaty that would place even more unbridled power in Brussels.

This recent Directive mandating data retention by internet service providers, combined with the extensive personal data on Europeans to be transferred to the US under the PNR and thereby set free to roam along the free market highways of North America do not paint a happy picture of personal data protection under European law.

It would seem clear, from a perspective of fundamental rights, particularly in light of the fact that such limitations on access to personal data arose directly out of one of the most horrific periods of state excesses in the history of Europe, that at a bare minimum legislation to reduce protection should only be undertaken unanimously (which is required at the EU level, unlike single market competence that AG has found sufficient, which requires only a qualified majority). While the question posed in this ECJ case was a narrow one, i.e. can legislation

aimed at preventing crime by mandating the retention of personal data by private actors, be based on the competence to enact single market directives, the underlying question of whether Europe still supports fundamental rights to data protection and privacy is paramount.

In an era where EU member states, most notably but not exclusively, the UK, are taking measures that invade the privacy of individuals to a degree inconceivable even two decades ago (including a national closed-circuit TV system estimated to photograph each UK inhabitant at least 300 times a day, with the suggestion that microphones be added in the near future, and the abovementioned proposed national database under which data is acquired without suspicion of wrong-doing or even the knowledge of the subject), individuals across Europe would be justified in expecting that their unelected officials in Brussels would at least make a show of protecting their rights, if only by refraining from duplicating these measures. Even if the European Court of Justice wisely rejects the AG's interpretation of EC competence to mandate data retention, and hold that only the EU has such power under the third pillar, subject to unanimity and on condition of the enactment of protection currently lacking in the EU legal structure, it would still be questionable state action from the perspective of fundamental rights developed over the past half century.

It is encouraging that the European Data Protection Supervisor has recently issued an opinion putting forth yet again his worries and suggesting the installation within the EU legal system a set of guarantees to compensate for the lack of a comprehensive legal framework on data protection in the field of cooperation between police and judicial authorities. But the forces, internal as well as external, in favor of reducing personal data protection are formidable.

"National security" and the "War on Terror" have taken the entire western legal order into dangerous territory in terms of reversing advances human rights law has made since its inception after WWII. Even in the United Kingdom, which all agree has the most pervasive system of privacy-invading technology on the planet, no reduction in criminal activity has been noted since these measures were instituted. Initially designed to weed out 'terrorists', this movement now feels justified to undertake full-scale surveillance over all individuals. And it is not just the chilling effect of ubiquitous state surveillance that is at issue in these developments. Corporate economic interests, including but not limited to intellectual property holders, have 'caught the coattails' of (and quite possibly been one of the forces behind, but that is for another essay) this onslaught on privacy. Once the state has full access to our personal data, communicated or stored in our hard disks or held by internet service providers, no one is safe and given what we have seen over the past few weeks in terms of states' ability or will to guard the basic interests of their citizenry, there is no reason to believe that good faith will prevail.

Virginia Keyder teaches European Union law at Bogazici University and Sabanci University in Istanbul, Turkey.

November 10, 2008