Introduction

‘Fortress Europe’ is a misnomer. Often used pejoratively, it implies that the EU is inward-looking and protectionist in terms of trade and immigration. This chapter shows how the idea of ‘Fortress Europe’ has taken on a new dimension as e-governance and efforts to combat cyber- and cross-border crime have assumed prominence on the EU’s agenda over the past decade. It discusses how the concepts of ‘border’ and ‘border management’ have taken on new meaning and given rise to whole new areas of policy – including those loosely termed ‘e-policies’ – that few dreamt of when the Single Market was in development. First, it is important to understand that the concept of ‘border’ has a traditional territorial, geopolitically defined meaning that permeates much of the debate about managing borders, especially with regard to the EU’s common external geopolitical borders. However, ‘border’ can also be understood in terms of virtual borders or, more accurately, access points to online services. Because access itself is increasingly designed to be facilitated by digital tokens, the wider debate in the EU (as elsewhere) has become rather muddled and, predictably, various directorates in the EU Commission and different government departments have failed to develop a coherent, strategic overview, with the result that contradictions abound. In the EU, for example, one institution concentrated on realizing an e-payments area, whilst others focused on research, e-passports and the multiple technical and political problems associated with facilitating cross-border information exchanges, the remote management of territorial borders (for example using drones) and externalized pre-border checks (as seen at Eurostar terminals and consular offices in third states). This chapter will briefly outline the policy evolution with respect to e-borders used to manage flows of people as well as e-borders conceived as access control to online services.

Cross-border cooperation intended to combat the illegal movement of goods, persons, services and capital has stimulated institutional and constitutional changes. By the time of the Lisbon Treaty negotiations, the transformational impact of information and communication technologies on policy across the board had been recognized, but the logical consequences for joined-up decision-making at all levels of government (not just the supranational) had yet to be adequately addressed. Consequently, the EU suffered from the same truncated thinking and piecemeal approach to the adoption of technologies to realize its policy goals that bedevilled national and
local governments. Inevitably, part of the problem lay in the financial constraints arising from
the banking crisis and subsequent recession across most of Europe. Another part arose from the
lack of understanding among policy-makers and officials about how the concept of ‘border’
had shifted from a territorial focus linked to the geophysical boundaries of a state to a functionally
determined conception.

The importance of mobile technology and the idea of citizens as ‘transhumans’ (i.e. people
whose lives are facilitated and monitored, ubiquitously and incessantly by mobile phones) have
begun to be recognized, but legislative responses to protect individual privacy and ensure
accountability have been out of sync with the realities of online lives, both in the EU and at
all levels within the member states. Paradoxically, the areas in which concern over the
preservation of national sovereignty had been most acute in the past – foreign affairs, defence
and internal security – were responsible for generating recognition of how cross-border inform-
ation sharing, not simply by those involved in combating crime, could have far-reaching impacts
on the lives of ordinary citizens. The concept of ‘Fortress Europe’ was reconfigured as the EU
embarked on a process of seeking acceptance for measures designed to protect its citizens’ digital
‘identities’ and ‘information’, wherever in the world the data was handled. The EU has
attempted to set standards that commercial interests and certain countries, including the United
States of America, have found challenging as all parties seek to exploit the economic advantages
presumably associated with online commerce and automated cross-border information exchange.

The chapter begins by outlining and contextualizing the origins of ‘Fortress Europe’ and the
Four Freedoms of the Single Market. It then provides an overview of how realizing the freedom
of movement of goods, persons, capital and services has had an unanticipated deepening effect
on European integration and how technological advances in information and communication
have transformed the scope of the integrative endeavour, the understanding of the importance
of EU values and rights, and the relevance and nature of territorial and virtual borders. This
has been especially evident in the highly sensitive domains of justice, freedom and security. The
chapter concludes with a review of the unique EU approach to border management,
demonstrating that through this approach, not only has the EU invigorated the debate over the
nature of privacy and security for EU citizens, but it has also increased confidence in a European
approach to universal challenges. In the process, states wary of this EU approach have been
forced to take Europe seriously. Dubbing the perspective ‘Fortress Europe’ is both misleading
and unhelpful: if the EU can produce a functional European model, people everywhere stand
to benefit.

From the piecemeal and truncated strategies of the various Commission DGs dealing with
the Four Freedoms, a more coherent approach to the movement and handling of digital data
is beginning to emerge, whether these data are used for commercial, behavioural, advertising,
tracking, personal or policing and security purposes. On the inaugural European Data Protection
Day in 2007, then-Commission Vice-President Frattini warned that in an era of globalization
in which information can circulate around the world in a flash, ‘we need to balance access to
data for those protecting our security and fighting crime with protecting people’s privacy rights.
This is not a balance which stands still. Rather both sides are able to move forward with
 technological advances’ (Frattini 2007). Directive 95/46 ‘on the protection of individuals with
regard to the processing of personal data and the free movement of such data’ (dubbed the Data
Protection Directive) was adopted to advance the Single Market by facilitating the convergence
of member states’ various regimes. This Directive established core principles with regard to ‘data
controllers’, lawful processing, the collection of data for explicit, defined and legitimate purposes,
and individual consent for processing. Exceptions from general requirements were authorized
for various reasons, including national security, defence and crime.
In 2013, this Directive was revised and transformed into a Regulation, in part to accommodate technological advances, bolster privacy protection and strengthen obligations regarding the processing and handling of EU citizens’ data anywhere in the world, and in part to ensure more uniform, predictable and dependable implementation by the EU28+. The proposed amendments provoked sharp accusations of a new ‘Fortress Europe’ from third states (including the United States of America) whose conception of privacy differed significantly from that of the EU; these contrary views regarding the priority that should be attached to ‘privacy’ clashed dramatically with the EU’s perspective, leading to a flurry of intense lobbying and amendments to the draft Regulation by third parties. By the end of 2013, the revision of this ‘Single Market’ legislation had acquired special importance, as the espionage scandal over US activities vis-à-vis its European allies threatened to derail the incipient transatlantic free trade agreement and compromise information-sharing practices (see Euractiv 2013a) such as the Terrorist Finance Tracking Programme (TFTP), the Passenger Name Record system (PNR) and the SWIFT banking agreement.

The diplomatic furore over Edward Snowden’s allegations of US spying on allied governments, including the tapping of German Chancellor Angela Merkel’s mobile (cell) phone,1 underlined the tensions confronting these governments within and outside the EU; in the name of Western liberal democracy, these countries must seek to maximize the transparency and accountability of their governments, while simultaneously strengthening security by adopting technologies that they hope will enhance their capacity to identify, predict and avert risks and threats.

In the EU, the concept of striving for a balance between privacy and security gradually gave way to the acknowledgement that certainty is impossible and privacy and security are part of a continuum: at times, exceptions to transparency (even involving intrusions into privacy) may be warranted in order to avert disaster. The EU Commission, in its executive rather than its bureaucratic role, attempted to demonstrate its willingness to listen to what citizens wanted (including anyone responding to its requests for feedback on initiatives). With the imminent expiration of the Stockholm Programme (‘An Open and Secure Europe Serving and Protecting Citizens’, 2010–14), it elicited opinions about what the future focus should be for its recently divided justice and home affairs directorates. Continuing the approach of the Tampere Process (Statewatch 2003) and the Hague Programme on these matters, it stated:

An internal security strategy should be developed in order to further improve security in the Union and thus protect the lives and safety of citizens of the Union and to tackle organised crime, terrorism and other threats. The strategy should be aimed at strengthening cooperation in law enforcement, border management, civil protection, disaster management as well as judicial cooperation in criminal matters in order to make Europe more secure. Moreover, the Union needs to base its work on solidarity between Member States and make full use of Article 222 TFEU.

(OJ C 115/5, 4 May 2010) (see Box 7.1)

‘Fortress Europe’: origins and context

The term ‘Fortress Europe’ was coined in the late 1980s, just before the nine-member European Community began a process of enlargement that would double and then triple the number of member states. ‘Fortress Europe’ was a term used somewhat pejoratively by third states and parties worried about the European Community’s internal efforts to boost its international economic competitiveness. These efforts centred on: (1) the removal of internal physical, financial
Box 7.1 The development of justice and home affairs cooperation in the European Union

Shortly after the UK referendum on remaining in the EEC, the European Council met in Rome on 1 December 1975 and agreed to enable meetings among ministers in the highly sensitive fields of justice and internal security; this was politically problematic, given the rhetoric surrounding sovereignty and the EEC’s limited policy competences. The TREVI Group was named after the Roman fountain where officials first met on 29 June 1976 at the ministerial level to discuss combating terrorism (from within the EEC states as well as international terrorism) but was also an acronym for their responsibilities: Terrorism, Radicalism, Extremism and International Violence; it explored potential information exchanges on terrorist threats and complementary strategies between member states whose approaches to defining terrorism and facilitating extradition differed. The group met thereafter outside the framework of the European treaties. In 1985, the TREVI Group’s remit was extended to illegal immigration and the fight against organized crime. The TREVI Group laid the foundation for the Single European Act’s Justice and Home Affairs (JHA) policy and pillars, particularly in matters of counter-terrorism (TREVI I), police cooperation (TREVI II), the fight against international crime (TREVI III) and the abolition of borders (TREVI 1992). See Lodge (1981, 1988) and Council of the European Union (2005a).

The Tampere Process originated in Title VI of the Treaty of the European Union (TEU) and Title IV of the Treaty of Amsterdam (TA), setting new objectives for justice and home affairs on policing, customs, legal cooperation, visas, immigration and asylum. An ‘Action Plan establishing an area of freedom, security and justice’ listing 51 specific objectives with target dates of two and five years was then adopted at the December 1998 European Council in Vienna (sometimes called the ‘Vienna Plan’). The Vienna summit at the end of the Austrian Presidency in 1998 agreed to put JHA at the centre of the EU agenda, in the same way that the original customs union, the internal market and, more recently, the common currency had previously been prioritized. Three core issues dominated the 1999 Tampere summit meeting: (1) a strategy paper on migration and asylum; (2) the Action Plan/Vienna Plan; and (3) the high-level group report and action plans on six target immigration ‘producing’ countries. For a critical examination of the process, see Statewatch (2003), the Hague Programme (Council of the European Union 2005b). The Hague process led to the Tampere agreement and set out priorities up to 2009, when it was succeeded by the Stockholm Programme (Council of the European Union 2010), with additional priorities implemented through an action plan. The Stockholm Programme began by asserting the commitment to protecting citizens’ rights inside and outside the EU, as outlined in the EU Charter of Fundamental Rights (European Commission 2013b) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe 1950/1998/2010), to which the EU acceded under the Lisbon Treaty that entered into force on 1 December 2009. It also noted that citizens’ right to privacy was to be respected, especially in terms of the protection of personal data.

In October 2013, the European Commission acted to improve EU-wide prosecution of financial crime by establishing the European Public Prosecutor’s Office, an independent institution subject to democratic oversight. It also proposed a reform of the European Union’s Agency for Criminal Justice Cooperation (Eurojust) and presented a Communication on the governance of the EU Anti-Fraud Office (OLAF) (European Commission 2013c).
and fiscal borders (seen as barriers to competition) among member states to facilitate the realization of the Four Freedoms of Movement — of persons, goods, services and finance — allowing the creation of the Single European Market by 1993; and (2) the consolidation of the external border around the territory of the Single Market. The removal of internal borders was designed to minimize technical and non-trade barriers and to reduce the bureaucratic requirements arising each time goods or people crossed the member states’ internal borders within the territory of the EU as a whole. Some powerful states outside the Single Market saw this as a potential threat to free trade. ‘Fortress Europe’ was thus used in a derogatory sense by parties anxious about: how these efforts might impact their international market share; increasing EU competitiveness; deeper European integration, including steps towards monetary union (such as the European Currency Unit (ECU) and subsequently the single currency); and the shift towards a common (but not single) foreign and defence policy, which was hinted at in the 1985 Milan summit declaration presaging the Single European Act. Ten years later, the EU had become much larger and more extensively integrated and was coming under increasing external pressure to integrate its internal security policies.

The EU’s member states eventually acceded, constitutionally and operationally, to the development of a common response on the international stage. The idea that the EU should speak with a ‘common voice’ seemed attractive to outsiders anxious about the diverse and sometimes conflicting policy statements and goals enunciated by member state officials, the EU Commission and the burgeoning number of agencies and politicians with an interest in what were loosely regarded as ‘foreign’ or ‘external’ affairs.

The disingenuous separation between the two during the EEC’s early years was clearly untenable. However, for many years, the implications for member states’ sovereignty, primacy and autonomy in international affairs arising from the EU’s development of its own ‘foreign policy’ (with the attendant personnel and remit), seemed a step too far. International events compelled a rethink of this stance. Incrementally, the EU developed a greater capacity to speak and act internationally with a ‘common voice’ (though not necessarily a ‘single voice’). Aspects of defence, policing, border management and civilian aid resources were deployed in accordance with the EU’s affirmed image as a ‘civilian power’ devoid of military might or territorial ambitions. Resources were marshalled to allow the EU to provide civilian disaster relief and member states to contribute to peacekeeping in line with UN decisions. In parallel with increasing capacities, a more logical and coherent approach to providing regional and international assistance and responses evolved.

In the course of these developments, a bevy of border management units and EU agencies emerged. Bodies such as Europol, the European Border Surveillance System (Eurosur) and Frontex (the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union) were the result of early steps towards cross-border cooperation with the purpose of combating international terrorism and organized crime (especially drugs, illicit goods and human trafficking). Operationally, this led to cooperation among the relevant member-state authorities (internal security, migration, customs, tax and police) to shore up the ‘leaky’ weak points in the EU’s ever-expanding external borders, especially to the east (see Box 7.2).

The Customs Information System (CIS) (European Commission 1992) and the European fingerprint database (Eurodac) were created relatively early on. Changes in their remits are regularly reviewed; most recently, the proposal to allow police access to Eurodac was condemned by the European Data Protection Supervisor (EDPS) in 2012 as mission creep, since this would overstep the purpose limitation principle. However, it should be noted that close cooperation on a bi- or multilateral basis among core EU states (reminiscent of the Kangaroo Group that
Box 7.2 Border management bodies in the European Union

The Convention establishing Europol under Article K3 of the Maastricht Treaty was agreed upon in 1995; after ratification by the member states, it came into force on 1 October 1998. In 1997, the Treaty of Amsterdam was signed, amending the 1992 Maastricht Treaty on the European Union. In the new Treaty, the EU’s ‘third pillar’, justice and home affairs, was pared down to focus on police and judicial cooperation in criminal matters. Its overall aim was to create ‘an area of freedom, security and justice’. The Treaty of Amsterdam incorporated the Schengen Agreements into EU law. The two Schengen Agreements of 1985 and 1990 became part of the EU’s *acquis communautaire* and were signed by all EU-15 countries except the UK and Ireland, and by two non-EU states (Iceland and Norway), with the aim of facilitating police cooperation in order to apprehend criminals fleeing across borders to avoid prosecution. The European Council in Tampere, Finland, in October 1999 progressed this. As a first step, the Council’s conclusions called for *joint investigative teams* (JITs) to be set up without delay to combat trafficking in drugs and people, as well as terrorism. JITs later became pivotal in Europol’s activities. The Tampere European Council strengthened Europol, established Eurojust to improve judicial cooperation and created the European police chiefs task force to coordinate policing at the operational level. Europol became fully operational on 1 July 1999 and evolved thereafter to deal with ever more serious threats; these developments included the Hague Programme’s intelligence-led law enforcement efforts at the EU level through the new *Organised Crime Threat Assessment* (OCTA). The Europol Convention, which came into force on 1 October 1998, provided the legal basis for Europol. Europol is not a ‘classic’ EU agency, as it was founded as an international organization with its own legal *acquis*, funded directly by contributions from EU member states. The Convention was amended three times by protocols, all of which entered into force in 2007. The Council then decided that the organization should be EU funded; after legislative changes were approved, this change came into force on 1 January 2010, when Europol became an EU agency and moved to new premises in The Hague (for more detailed information, see Europol 2014).

On 2 December 2013, the *European Border Surveillance System* (EUROSUR) became operational. This system is designed to enhance the capacity of member states to coordinate actions to detect, prevent and respond to illegal immigration using appropriate technology; it also seeks to improve inter-agency cooperation among the relevant states. Eventually, EUROSUR will be operational in 30 countries in total. In the initial phase, it became operational in 19 countries (the 18 EU member states at the southern and eastern external borders and the Schengen-associated country Norway). On 1 December 2014, the remaining 8 EU member states and 3 additional Schengen-associated countries will join EUROSUR. Ireland and the United Kingdom are not full members of the Schengen cooperation and therefore will not participate in EUROSUR. The EUROSUR Regulation states that all parties must comply with the principles of non-refoulement and human dignity when dealing with persons in need of international protection. EUROSUR is restricted to operational information, such as the location of incidents and patrols, and only very limited exchange of personal data was envisaged.

The origins of the *European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union* (Frontex) lie in the advances in border management cooperation of the 1990s, particularly the creation of the External Border Practitioners Common Unit – a group composed of members of the Strategic Committee on
Immigration, Frontiers and Asylum (SCIFA) and the heads of national border control services. This unit coordinated national projects on border control through Ad-Hoc Centres (Risk Analysis Centre, Helsinki, Finland; Centre for Land Borders, Berlin, Germany; Air Borders Centre, Rome, Italy; Western Sea Borders Centre, Madrid, Spain; the Ad-hoc Training Centre, Traiskirchen, Austria; Centre of Excellence, Dover, UK; and Eastern Sea Borders Centre, Piraeus, Greece). Two years later, in October 2004, the European Council created Frontex with Council Regulation (EC) 2007/2004 (Frontex 2014).

Box 7.3 Information systems in the Schengen Area

The Schengen Information System (SIS) was established as an intergovernmental initiative in parallel with the push to realize the Single Market. The 1985 Schengen Agreement to facilitate freedom of movement was limited to seven member states. This was superseded by the wider 1994 Schengen Convention, which is now integrated into the EU framework. SIS may be accessed by law enforcement, customs and tax authorities for the purposes of combating crime and illegal entry to the EU. It also coordinates alerts on missing persons (in particular children) and lost or potentially stolen property, including weapons and identity documents. National authorities enter information into SIS. SIS II, one of the world’s largest IT systems in the field, consists of three components: a Central System, member states’ national systems and a communication infrastructure (network) between the central and national systems. The so-called SIRENE Manual lays down the procedures for member states’ exchanges of supplementary information on alerts stored in SIS. Further details are available at European Commission (2013a).

Since October 2011, the Visa Information System has allowed Schengen states to access visa information with a view to combating visa-shopping, fraud and related crime. Details are available at European Commission (2013a).

Members of the Schengen Area include the non-EU states Iceland, Liechtenstein, Norway and Switzerland, as well as most EU members, except Croatia, Cyprus, Bulgaria and Romania (whose domestic arrangements are not yet sufficiently robust against corruption, according to EU Commission reports) and Ireland and the United Kingdom (who opted out but have special provisions) (European Commission 2013a).

Passenger Name Record (PNR) data refers to information collected during the reservation and booking of aeroplane tickets and when passengers check in for flights, as well as that collected by air carriers for their own commercial purposes. It includes several different types of information, such as travel dates, travel itinerary, ticket information, contact details, the travel agent through which the flight was booked, the means of payment used, seat number and baggage information. The data is stored in the airlines’ reservation system and departure control databases. For details, see European Commission (2014a).
Even before the push to consolidate and reinforce a common external border around the EU, member governments had recognized their inability, both individually and as a group, to devise and implement appropriate and timely policies to ensure their territorial security and the safety of European citizens in the face of international organized crime and, increasingly, cybercrime. However, mutual mistrust, the legacy of communist and totalitarian practices, and differences in the understanding of the Western concepts of democracy and the ‘rule of law’ meant that the rhetoric of cooperation and information-sharing was repeatedly tested as the integration of border management and policing progressed. Successive Commission reports as late as 2012 stated that the deficiencies of Romanian and Bulgarian judiciaries and law enforcement were so extensive that the countries’ exclusion from full participation in information-sharing arrangements related to judicial cooperation and internal security was warranted (European Commission 2014b).

One of the most intriguing facets of integration has been the pace of EU cooperation in judicial and internal security matters. In this arena, the concept of borders was first reconfigured politically, as the realities of policy-making and operational successes struck home, and then again as technology transformed the capacity of those implementing the policy to work together in real time. The reasons behind this development are briefly explained below.

**Issues**

Both external and internal security were traditionally seen as *bêtes noires* by member governments; as the cornerstones of national sovereignty, they were initially excluded from integration. However, even the profoundly intergovernmentalist, Eurosceptic Thatcher administration in the UK advocated ‘cooperation’ in these fields, whilst vigorously opposing supranational economic integration, the single currency, the extension of the European Parliament’s legislative power and any expansion of the policy scope of the EU (Thatcher 1988). Cooperation on the intergovernmental model favoured by the British became a stepping stone to broadening the scope of integration, persuading other states keen on retaining national autonomy of the need for greater cooperation, if only to ensure that Europe’s relative political power on the world stage did not sharply decline. This marked a profound change in approach that led to ‘soft law’ measures expanding the scope of integration in ways few would have previously imagined possible. The Single Market’s soft diplomacy (creating a form of civic identification with the European project) was slowly realized through the People’s Europe agenda of 1985 (Adonnino 1985). This step had been alluded to in the references to the creation of a human union that were made when Denmark acceded to the European Community in 1973. This was transformed into the concept of active EU citizenship, reminiscent of the functionalist theory of socio-psychological community formation (identity and self-identification with Europe). Originally, it was designed to complement and reinforce national citizenship by means of common socio-economic and political rights, including the right to contest and vote in European Parliament elections. This right was first set out in the 1957 Treaty of Rome that founded the European Economic Community, but it was only realized in 1979 after intense squabbling over its implications for national sovereignty and the position of national governments at the apex of European political structures following the direct election by universal suffrage of Members of the European Parliament (Herman and Lodge 1978; Corbett 1993).

During the 1990s, the Commission set up a High Level Panel on the free movement of persons in order to map practical, legal and administrative barriers; its conclusion was that obstacles resulted from indirect discrimination.² By the turn of the century, EU citizenship guaranteed...
Box 7.4 The European Citizen Action Service

The European Citizen Action Service hotline is a tool designed to demonstrate to EU citizens that the EU is responsive to their needs, notably with respect to the exercise of the Four Freedoms. Similar initiatives include Europe Direct, which was established to answer citizens’ questions about the EU, and the European Judicial Network (EJN) for civil and commercial matters; the European Commission manages the EJN website at EJN (2014). This system was designed ‘to make access to justice easier for all Europe’s citizens’, according to the Commission’s statement in 2003. See its publications Civil Law at Your Fingertips (2003) and Practice Guide for the Application of the New Brussels II Regulation (on the courts responsible in divorce-related matters) (2005) at European Commission (2014b).

A decade ago, the prevailing idea that internal and external security could (and should) be separate domains was challenged by the freedom of movement enjoyed by international organized crime, rising illegal immigration, human trafficking, international terrorism and cybercrime. Those charged with operationally combating threats to internal and external security had engaged in bi- and multilateral cooperative efforts in order to detect, apprehend and prosecute criminals across domestic, regional and local borders as well as international borders. However, the absence of uniform arrangements meant that intra-EU differences could be exploited to the EU’s disadvantage. Around the turn of the century, initiatives seeking to overcome this deficiency were given additional impetus by third states (especially the US) and the increased risks arising from regional wars in Africa, the Middle East and Afghanistan (Hill and Smith 2000; European Commission 2001).

Internally, earlier efforts at cross-border cooperation to combat international crime had led to advances in policing, customs, immigration and judicial cooperation, including the cross-border exchange and sharing of information. The European Drugs Monitoring Unit evolved into Europol, and within a decade several new agencies had been established to deal with cross-border issues and manage (predominantly territorial) borders. These included Frontex and the European Fundamental Rights Agency (FRA), as well as the plethora of EU committees working to develop policy initiatives on asylum, immigration, racism and civil defence. In 2010, a special cybercrime unit was belatedly established. By 2013, following the Prism surveillance revelations and special enquiries launched by the European Parliament and European Commission (echoing earlier debate over the Echelon Interception System in the European Parliament’s Temporary Committee on the interception of private and commercial communications in 2000), some governments had begun to advocate a coherent approach to the management of domestic and commercial digital services, including the imposition of a common digital tax to fund development.
Theories: from securitization and surveillance to the primacy of ethics

The dominant theories related to ‘border’ management can be divided into the categories of surveillance and securitization, both of which are nested in theories of international relations – for example the diverse security-related theories such as those of the Copenhagen School (critical security) and the Welsh School (emancipatory realism). Surveillance is dominant among criminologists interested in policing and profiling, and among sociologists focusing on the organization of society; however, the literature is too extensive to review here. By contrast, EU theories of integration suggest that federalism is signaled by shifts towards common policies in defence, security, foreign affairs, currency and finance (Cameron 1999; Burgess 2000; Hill and Smith 2000). With the 2000 Treaty of Nice, the federal spectre began to worry member states, especially after the 2002 Convention on the Future of Europe and the European Council meeting in June 2003 in Thessaloniki advocated establishing a constitution for Europe.

EU theories of integration are helpful in conceptualizing the gradual steps in the development of the EU’s competences in certain aspects of internal and external security. Equally, however, EU law reflects the problems of edging towards common rules at a time when the union was swiftly expanding to encompass regimes with sometimes contradictory laws, traditions and values.

In general, the primary tensions in EU deliberations identified by research on its ‘homeland security’ and ‘security pillars’ are due to operational disagreements over the nature of the ideal balance between privacy and safety and between liberty and security, respectively (Guild 2004; Balzacq and Carrera 2007). The notion of exceptionalism – that is, making exceptions to the general democratic principles of governmental accountability, openness and transparency – has been used to track creeping infringements on privacy and liberty in the name of security (Bigo et al. 2010). Deviations signal an erosion of democratic legitimacy. Security is the one area in which exceptions (secrecy, and all that is implied to maintain secrecy) to the general principle of openness have been traditionally justifiable on the grounds of national security interests.

Over recent years, the fear that new technologies deployed in what are regarded as public spaces (such as shopping districts, public parks, streets, railway stations, hospitals, schools, public transport systems, etc.) are progressively invading and compromising the individual’s capacity to remain anonymous and ‘private’ has grown. Governments and private companies have employed CCTV, face-recognition analytics and real-time monitoring of public spaces, thereby exploiting and commercializing data – unpicking, analysing, linking and decoupling it from the original purposes for which it may have been provided or gathered. The innovations facilitated by new technological applications have raised particular concerns with respect to their use by state authorities. The greater ‘informational power’ arising from technologies that could be used or exploited for surveillance and monitoring, under all manner of pretexts by all manner of bodies, has provoked a degree of disquiet with regard to their purpose. This was most evident in the public sector when governments extended the number of policy areas subject to ‘exceptional’ rules allowing them to avoid the usual transparency and accountability provisions associated with parliamentary and public scrutiny of government on the grounds of ‘security’. This had been the norm where threats to national security were concerned, and it was typical in foreign affairs, but it became problematic as ‘exceptionalism’ crept into domestic politics. Theorists refer to this expansion as ‘securitization’. Justified by governments largely on the basis of the growing threat of international terrorism, such measures have proliferated, leading to the concern that new technologies will allow a Panopticon Big-Brother state to evolve, eroding...
personal privacy and legitimating pervasive surveillance. Theories of surveillance have proliferated. Lyon has defined surveillance as ‘any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered’ (Lyon 2001: 2). Brey notes that ‘Surveillance frequently undermines privacy because its very purpose is to retrieve information about persons and use it to exert some amount of control over them, and surveillance often takes place without informed consent’ (Brey 2005).

The transformative impact on society of digital traces that allow citizens to be trackable any time and anywhere has been probed by social scientists and criminologists alike. Here, the digital persona is viewed as an algorithm that can be used to classify, profile, distinguish and categorize people; it can predict and perhaps forecast, reward or prescribe certain behaviours and categories of people in defined spaces. Lodge refers to this idea as ‘quantum surveillance’ (Lodge 2010b) and has shown how this raises numerous issues of accountability, control, transparency, legitimacy and ethics (Lodge 2012c). The permeability of spaces and the invisibility of the people and computers handling personal data and making automated decisions based on predefined criteria and manipulable mathematical formulae have raised acute concerns with regard to European values, the nature and meaning of identity, responsibility, fundamental rights, autonomy, human dignity, what it means to be human, the role and rights of machines, and how governments and authorities entrusted with protecting citizens and their rights can fulfil this task as boundaries become reconfigured and infinitely malleable (Lodge 2011, 2013a).

A growing interest in the impact of information and communication technologies across all realms of activity in society has led to a focus on the ethical dimensions of the use and purposes for which such technologies could be employed (van Steendam 2005; Lodge 2010a, 2010b, 2012c, 2012d, 2013a, 2013b). The transformative impact and relevance of the guiding principles of medical ethical codes are mirrored in contemporary EU data protection and privacy deliberations. These include: the precautionary principle, purpose minimization, purpose specification, purpose limitation, proportionality, necessity, informed consent, data integrity, legitimate use and the slippery concept of a duty of care. The increasing use of biometrics for identity management has precipitated an exchange on ethical issues between social scientists, computer engineers and industry that goes beyond the concerns over secure and robust data-handling practices (many of which remain woefully lax, as national data supervisory authorities confirm), the costs of redress and the commercialization of ‘security technologies’ for domestic use, such as automated facial recognition, near-field communication and other tracking and robot-based technologies. The principles of ‘privacy enhancing technologies’ and ‘privacy by design’, intended to ensure that safeguarding the security and privacy of a citizen using an information and communication (ICT) device would be ‘baked in’ ab initio, finally began to gain currency after over a decade of academic research, briefings to and from the Civil Liberties Committee of the European Parliament and strongly worded opinions from the European Data Protection Supervisor’s Office (Lodge 2012a, 2012b; Mordini and Tzovaras 2012; Rommetveit and Gunnarsdóttir 2013; Warwick 2013).

Beginning in 1991, the EU’s high-level European Group on Ethics in Science and New Technologies (EGE), one of the first such ethics committees in the world, stressed the need for vigilance in the face of risks arising from the instrumentalization and merchandizing of the human body, all of which were reflected in the EU Charter of Fundamental Rights. This coincided with the Delors White Paper (European Commission 1993), which emphasized the need to develop infrastructure to respond to globalization. The significant big-business influence on the Bangemann Report and the Commission Action Plan in 1994 (European Commission 1994) culminated in the eEurope 2002 targets, which were designed to facilitate the introduction
of a knowledge-based (computer-driven and ultimately) online information society, first recognized by the Commission in 1979 (Gomez-Barroso et al. 2008: 797).

The European strategy promoting the information society, known as the eEurope programme, ended in 2005 with the launch of the i2010 programme (Gomez-Barroso et al. 2008). Significantly, in 2005 the EGE’s new mandate underscored the need for its independent polymath members to advise the Commission on the ethical aspects of new science and technologies. As society was transformed and digital personae came to be seen as multiple, distributed systems transmitting and receiving information and as an inexhaustible source of new information (Rodata 2005: 41), norms and values (such as respect for pluralism and diversity) that had been taken for granted as the basis of an EU founded on the Four Freedoms, the rule of law, justice, tolerance, dignity and equality were challenged. Capurro has identified a new principle of freedom in the twenty-first century, asserting that ‘freedom of access becomes a key ethical issue of the so-called information society’ (Capurro 2005: 22). Balancing that access in the evolving landscape of sometimes very sensitive personal information flows and changing human capacities remains problematic, as does ensuring the ethical use of information.

The Treaty of Lisbon entered into force in 2009. It set out a Europe of rights and values: human dignity, freedom, democracy, equality, the rule of law and respect for human rights. It also guaranteed the enforcement of the 2001 Charter of Fundamental Rights (European Commission 2013b). Both the first President of the European Council Herman Van Rompuy (in his first speech on 19 November 2009) and Commission President Barroso (in his February 2010 speech to the European Parliament) emphasized the entrenchment of these rights and values in the EU’s core design (EGE 2010: 18–19).

Among these hard-won freedoms and rights, privacy achieved new prominence and currency in an unexpected way in 2013, at a time when the old idea of ‘Fortress Europe’ was receding with the increasing consolidation of the transatlantic region. It was the European concept of ‘privacy’ that shook this, once again leading to accusations that Europe was acting as a ‘fortress’ by isolating itself with restrictive practices (in this case, strong adherence to making privacy a personal reality rather than a commercializable commodity). These practices were denounced by more ‘liberal’ state and private bodies with different views about the priority and interpretation of moral values, ethical data-handling procedures and ensuring and maintaining the right to privacy in the hierarchy of rights. Underpinning this perspective, however, was a growing conviction that the EU’s freedoms and fundamental rights were more than merely rhetoric. The EDPS (a post established in 2001), Peter Hustinx, succinctly expressed the complementarity – as opposed to the contradictions – between protecting data privacy and promoting the Single Market’s Four Freedoms: ‘Arrangements for data protection must as far as possible actively support rather than hamper other legitimate interests (such as European economy, the security of individuals and accountability of governments) . . . A fundamental right aims to protect citizens under all circumstances’ (Hustinx 2012: 33).

Rhetoric and reality: deeper and newly contested integration

Missing from this debate was an appreciation of the intensification and deepening of European integration that were precipitated by common actions to manage territorial and virtual ‘borders’. Even before the turn of the century, EU governments had introduced measures to facilitate information exchange for operational purposes connected to policing and the related sensitive justice and home affairs areas. This quickly progressed to policies building on intra-EU bi- and multilateral cooperation, the Trevi agreements (the foundations of what later became Europol) to promote cooperation in the effort to combat terrorism (Council of the European
Union 2005a: 7), mutual legal assistance conventions, the Council of Europe conventions and international agreements with third parties. Security, asylum and immigration concerns in early 2001 presaged greater intra-EU cooperation via the EU’s high-level Committee on Immigration, Frontiers and Asylum (SCIFA) and increased collaboration with the United States, notably in terms of the definition of terrorism. At its extraordinary meeting on 20 September 2001, the EU Council agreed to expedite the creation of an area of freedom, security and justice (in subsequent elaborations this was known as the Tampere Programme, the Hague Programme and the Stockholm Programme) and to bolster cooperation with its partners, especially the United States, in order to improve and formalize (and rectify the often ad-hoc nature of) EU–US judicial cooperation in criminal matters, including the sharing of lost passport data and access to the VIS database (which had been established to allow Schengen states to exchange visa information) (European Commission 2013a)\(^6\) for the purposes of combating terrorism and other serious criminal offences (Bigo et al. 2010; see Boxes 7.1 and 7.3). In addition, there were changes made in the remits and resources of Eurojust and Europol. In 2005, the Prum Treaty, designed to improve police cooperation, including access to files for forensic purposes (e.g. the automated exchange of DNA and biometric data), was signed. Further developments in this area have included the European Police Records Index System (European Commission 2012), the Visa Information Exchange System (VIS, the most extensive cross-border system in the EU, covering applications for Schengen visas) and Eurodac (containing the personal and biometric information of all asylum seekers and illegal immigrants). The Schengen Information System (SIS I and SIS II, operational since April 2013) is intended to complement other relevant databases such as VIS, and can be revised in response to changing security needs. In reference to Schengen visa applicants, the EDPS cautioned in 2006 that ‘it is of utmost importance that data protection is taken seriously for these, a priori, innocent people’. He took a robust line vis-à-vis all proposed changes to the remits of EU agencies, including Europol (Hustinx 2006), and to EU–US information sharing. Governments have used a growing range of ‘soft law’ instruments, such as framework decisions (2008) – initially escaping public parliamentary control – to intensify this. These have included bilateral agreements setting minimal data protection guarantees by Europol (in 2001) and Eurojust, and the US (in 2006) with respect to the Passenger Name Record (PNR) agreements (in 2007), terrorist financing (in 2007) and the SWIFT system (which led to an exchange of letters between the EU and the US); in addition, there were agreements reached between the EU and Australia on the processing and transfer of EU-sourced PNR data to the Australian customs authority by air carriers.

The Passenger Name Record programme allowing US access to PNR data under the information exchange system proved highly controversial (see, for example, the criticisms of the British House of Commons Home Affairs Committee 2007); however, it had been foreshadowed by the informal US–EU Commission agreement in 2003 (authorized on 23 February 2003 by the Council), under which many EU air carriers allowed the US Customs and Border Protection department access to 40 data fields from the Amadeus database. This informed the later deliberations of the EU–US High Level Contact Group (HLCG) on information-sharing, privacy and personal data protection (2008). The EU Article 29 Working Party on Data Protection was highly critical of both Amadeus and the PNR system (2002). The EDPS heavily criticized these developments (2006), condemning the existence of data warehouses where information about non-suspected individuals would be stored with an eye to potential future needs. The EDPS took issue with the HLCG over exceptions that weakened the prohibition on the processing of sensitive data (EDPS 2008), and over the adequacy of the benchmarks ensuring sufficient protection of personal data (EDPS 2008: para. 41–4) proposed for future instruments. In particular, he insisted on compliance with international and European
legal frameworks and with the commonly agreed-upon safeguards enshrined in the UN Guidelines, Convention 108 of the Council of Europe and its additional protocol, the OECD guidelines and Directive 95/46/EC. The EDPS stressed that adequacy was protected under the first pillar through Article 25 of the Directive 95/46 but was not explicitly set out under the third pillar. In short, the impact of this transatlantic instrument on data protection was likely to include changes in the existing legal framework, fundamental rights, independent audits and oversight, transparency, redress, the accountability of law enforcement authorities and data retention justifications, with direct ramifications for citizens. As Hustinx noted, ‘The scope of public security remains unclear, and the extension of transfers in case of breach of ethics or regulated professions appears unjustified and excessive in a context of law enforcement’ (EDPS 2008: para. 80). Concerns over information exchange for ‘security’ and policing purposes (arising from efforts to prevent and combat terrorism as well as international crime) grew. Where direct issues could be addressed and disproportionate exchanges limited, action by legislators had some success. The European Parliament challenged the PNR arrangement before the European Court of Justice in 2004 and secured certain amendments after a bitter fight. In May 2010, Parliament postponed its vote on a PNR agreement with the US that had been applied provisionally since 2007, mainly due to data protection concerns. The European Commission, at the behest of MEPs, negotiated a new deal in 2011 that was subsequently approved without further reference to the Court. This agreement, which came into force following formal approval by justice and home affairs ministers, expires in 2014. PNR agreements with other countries, notably Australia and Canada, have also been negotiated.

Other important steps have included the informal agreement in 2007 to explore and later transpose the Prum Treaty into EU legislation, and the exchange of personal data (including biometrics, such as DNA and fingerprints, and motor vehicle data [Eucaris]) enabling the creation of a cross-border police information network to enhance activities combating cross-border crime. These measures were complemented by the introduction of automated border controls (such as the automated passport gates at various airports), biometric passports and common standards for security features and biometrics in travel documents (EC 2252/2004, Council of the European Union 2004a), pre-border checks (such as those at Eurostar terminals, procedurally modelled on the US CAPPS II and US-VISIT schemes) and out-sourced visa checks across the world.

National governments have jointly resourced and managed policies related to the information society, including: the creation of a supranational cybercrime unit and an EU cyber ‘tsar’ to unify and enhance EU responses to money laundering (later using the SWIFT agreement) and international crime; the strengthening of border management agencies (including Frontex and Eurosur); and the use of remotely controlled drones to help manage sovereign states’ borders (at times employing robots and technology also used for military and disaster purposes beyond the EU’s borders). However, the extent of mutual collaboration in the fields of internal (homeland) and external (foreign) security – traditionally viewed as uniquely the preserve of sovereign, autonomous governments – has been far from obvious, even though the European Security Strategy (2003) predicted intensified action in security and defence over ten years ago (European Commission 2004c). The terminology used is especially striking. Less than 20 years earlier, the idea of common security and defence was anathema to most governments, even as the Single European Act (1985) took shape, later evolving into the three pillars of the Maastricht and Amsterdam Treaties. Before 2001, the European Parliament had had to fight to gain access to the draft documents that formed the basis of legislative proposals. As its position changed, it obtained access to sensitive security information (2002). With co-decision now the norm, MEPs
have genuine legislative power and responsibilities vis-à-vis their electorates. All these significant developments were precipitated by the Single Market (see Chapters 10, 11, 13).

As the EU has expanded, older states facing increasing right-wing extremism and Euro-scepticism on the eve of the 2014 European Parliament elections have looked for ways to ‘roll back’ supranational ‘red tape’ and ‘federalism’ of the most centralized variety. The institutional and constitutional changes entrenched in treaties following the 2000 European Convention (changes related to the Charter and especially the 2002 Convention on the Future of Europe), culminating in semantic wrangles over the terminology used in what eventually became the Constitutional Treaty, were significant indicators of deeper integration (and federalism). The same can be said of the cross-border responses of political movements in the face of growing public disenchantment with the EU (exemplified by rising support for Eurosceptic and extremist elements) (Seoane Perez 2013) and with national governments in the wake of the financial crisis.

Social networking, crowd-sourcing and viral campaigning have facilitated these movements; the EU Commission, national governments and MPs and MEPs have joined in as part of an effort to ‘communicate Europe’ (Lodge and Sarikakis 2013). In practice, technology has transformed the original concept of ‘border’ as a barrier in the minds of those using these new applications. This applies to citizens voluntarily sharing all manner of personal information online (thereby arguably shrinking their private space) as well as to data miners, ad trackers, online behavioural monitors and governments eager to plough through and commercialize data. However, legal regulation has not kept and cannot keep pace with these developments (Nagel 2013). What is instructive in this regard is the EU Commission’s attempt to update the directive on data protection, as well as third parties’ vigorous campaigns to thwart the evolution of a single regulation in its place. For the latter group, this draft regulation in 2013 epitomized ‘Fortress Europe’. For the EU’s member governments dealing with the media fallout from the revelations of Prism surveillance, a more robust commitment to upholding and implementing the EU’s fundamental rights and freedoms on behalf of citizens was imperative.

There has been mounting evidence of the insecurity of online transactions, cybercrime, sloppy data-handling practices, cavalier disregard for privacy and the endangerment of vulnerable people and children as digital data is spliced, reconfigured, sold and re-sold, and used outside the original jurisdictions without the explicit consent of the individual concerned. At the very least, the EU and its member governments must give a strong legislative signal that they are on the side of citizens and the implementation of the law.

Conclusion

The concept of ‘Fortress Europe’ is seriously misleading in terms of the actual complexities of decision-making in highly sensitive policy fields in which there are numerous actors that include observers and participants from third states. Although outlining these structures is outside the remit of the chapter, it is important to note that the EU’s relative openness to third-state involvement challenges the notion that its internal decision-making is an impenetrable ‘fortress’. In times of crisis, the need for international cooperation has resulted in concerted efforts to work within and outside existing structures to mitigate problems. This applies most obviously to the struggles against terrorism, illegal immigration, goods and human trafficking, and core aspects of international organized crime. National governments’ commitment to maintaining their values, norms and politico-economic and socio-legal practices within their territorial borders have been challenged by the new technology of e-borders and the associated demands (from society and from the EU) to uphold the liberal democracy, representative accountability and
rule of law its citizens take for granted. The challenges for the future will entail reconciling these demands with accelerating technological advances that combine with and are integrated into the person and can be used for good or ill. This requires open-mindedness on all sides as well as a continuation of Monnet’s approach, enabling each generation to put its own considered stamp on European integration.

Notes

1 At the 24–25 October EU summit, Merkel demanded that the United States sign a ‘no-spying’ agreement with Berlin and Paris by the end of the year, stating that the alleged espionage against two of Washington’s closest EU allies had to be stopped. For details, see the dossier Euractiv (2013b).

2 Indirect discrimination means that a member government does not treat non-nationals with EU citizenship and its own nationals equally.

3 In July 2013, the European Commission said that it would report to the European Parliament and Council in October 2013 to discuss the findings of an expert group set up by the EU and the US following dialogue between Viviane Reding, the Commissioner for Justice, Fundamental Rights and Citizenship, and US Attorney-General Eric Holder. See Euractiv (2013c).

4 For a succinct summary of key theories relevant to functionalism and its successors, see Lodge (1993) and Burgess (2000).

5 The EDPS is entrusted with ensuring that all EU institutions and bodies respect citizens’ right to privacy when processing their personal data. Details about the role and remit are available at http://europa.eu/about-eu/institutions-bodies/edps/.


Bibliography


—— (2013), Note from the Politico-Military Group to the Political and Security Committee on PMG recommendations on the CSDP aspects of the Cybersecurity Strategy of the European Union. 25 March.


—— (2001), Governance in the European Union, Cahiers of the Forward Studies Unit, Brussels.


European Council (1999), Presidency Conclusions of the Tampere European Council, 15–16 October.


Juliet Lodge


European Parliament (2000), Regulation (EC) No 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies on the Free Movement of Such Data, 18 December.


‘Fortress Europe’


