UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

The SWIFT affair and the global politics of European security

de Goede, M.

DOI
10.1111/j.1468-5965.2011.02219.x
Publication date
2012
Document Version
Final published version
Published in
Journal of Common Market Studies

License
Article 25fa Dutch Copyright Act (https://www.openaccess.nl/en/in-the-netherlands/you-share-we-take-care)
Link to publication

Citation for published version (APA):
de Goede, M. (2012). The SWIFT affair and the global politics of European security. *Journal of Common Market Studies*, *50*(2), 214-230. https://doi.org/10.1111/j.1468-5965.2011.02219.x

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:14 Jun 2024

JCMS Journal of Common Market Studies UACES

JCMS 2012 Volume 50. Number 2. pp. 214–230 DOI: 10.1111/j.1468-5965.2011.02219.x

The SWIFT Affair and the Global Politics of European Security*

MARIEKE DE GOEDE
University of Amsterdam

Abstract

This article examines the 'SWIFT affair', whereby United States security authorities acquired access to financial data of European citizens, and argues that it is a powerful lens through which to understand current shifts in European security governing. The affair demonstrates the institutional challenges produced by the deployment of private, commercial data for security, and analyzes the ad hoc innovations produced in European Union (EU) governing as a result. Furthermore, the SWIFT affair has allowed the EU to position itself in the global security landscape as a normative power that promotes the values of privacy and data protection. However, the development of a European Terrorism Financing Tracking System, coupled with the way in which the EU itself is keenly implementing risk-based and data-led internal security measures, means that critical attention to the EU's own security practices remains urgent.

Introduction: The SWIFT Affair

In February 2010, Dutch Member of the European Parliament Jeanine Hennis-Plasschaert received a standing ovation in the European Parliament after it decided to reject the EU–US interim agreement that guaranteed to United States security authorities continued access to European financial data held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). This agreement had been reached at the highest levels of EU–US negotiation in order to secure American access to these data after SWIFT had closed its American data processing centre, and was strongly supported by the European Council and Commission. The reason why the European Parliament (EP) rejected the agreement was its continuing concerns over the privacy and security of the financial data of EU citizens made available to the United States. As Hennis-Plasschaert said in her speech prior to the parliamentary vote: 'Currently, our laws are being broken, and under this agreement they would continue to be broken'.[1] The vote resulted in a temporary halt to the transatlantic data transfer and a renegotiation of the terms of the agreement. A new transatlantic agreement, concluded in June 2010, includes enhanced stipulations

* Many thanks to two anonymous *JCMS* referees for their very helpful comments. I am grateful to my colleagues at the Politics Department of the University of Amsterdam, who offered their generous comments when I presented an earlier version of this article. Special thanks to Alexandra Hall and Mara Wesseling for research assistance. Funding for the research of risk-based approaches to targeting money and people is provided by ESRC (United Kingdom) and NWO (Netherlands). 'DataWars: New Spaces of Governing in the European War on Terror' (award no. RES 062230594) is conducted together with Louise Amoore of Durham University.

[1] Video material of the European Parliament's debate and vote is available online at: «http://www.europarl.europa.eu/wps-europarl-internet/frd/vod/player?language=nl&menusearchfrom=bymep&pageby=unit&idmep=28176&discussionId=0&page=0&category=0&format=wmv?date=&askedDiscussionNumber=2». The Hennis-Plasschaert quote is at 12:18:20, the standing ovation takes place at 12:25.

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd, 9600 Garsington Road, Oxford OX4 2DQ, UK and 350 Main Street, Malden, MA 02148, USA

concerning the protection of data and the rights of redress for citizens, and was duly approved by the EP (Council, 2010).

The EP vote and the June 2010 agreement were important new developments in a much longer political contestation over the availability of the SWIFT wire transfer data to American authorities in the context of the post-9/11 fight against terrorism. In October 2001 the United States Treasury, in co-operation with the Central Intelligence Agency (CIA), secured access to SWIFT data in the context of what it called the 'Terrorism Financing Tracking Programme' (TFTP). This programme was part of a larger post-9/11 turn to a risk-based deployment of commercial data for security purposes, and 'grew out of the Bush administration's desire to exploit technological tools to prevent another terrorist strike' (Lichtblau and Risen, 2006). The SWIFT data were analyzed with a view to identifying transactions, connections and networks of the 9/11 hijackers as well as other suspected terrorists and listed entities (Amicelle, 2011; Wesseling *et al*., forthcoming). The programme's objectives of identifying investigative leads and disrupting potential future terrorist activities must be regarded as part of a wider turn to a politics of banal pre-emption in the post-9/11 security landscape (Amoore and De Goede, 2008; Aradau and Van Munster, 2007; Anderson, 2010).

It was five years later in June 2006 that the existence of the TFTP was disclosed to the general public when the *New York Times* publicized the programme and assessed its implications in terms of the war on terror and civil liberties. The 2006 disclosure sparked substantial debate on both sides of the Atlantic, and caused a transatlantic controversy whereby the EP and European privacy commissions took the lead in criticizing the fact that American security authorities were given access to confidential financial data of European citizens held by a private company. In the face of these critiques, American authorities – under both the Bush *and* the Obama administrations – defended the programme in the strongest terms and pressed for its continuation. As American Vice-President Joe Biden said in a May 2010 speech to the EP: 'The longer we are without an agreement on the Terrorist Finance Tracking Programme, the greater the risk of a terrorist attack that could have been prevented'.[2]

This article examines the 'SWIFT affair', and argues that it is a powerful lens through which to understand the nature and shape of an emergent European security community. The SWIFT case is important to understanding the development of current EU security politics precisely because it demonstrates that the distinction between internal and external security becomes increasingly difficult to draw (Burgess, 2009). On the one hand, the SWIFT case reveals the contemporary institutional tensions and innovations caused by the deployment of private, commercial, data for public security purposes. The EP was initially sidelined because the issue was cast as a third-pillar (internal security) measure, over which it has little say. However, after the coming into force of the Lisbon Treaty in December 2010, the SWIFT affair became the first manifestation of the EP's new powers in the security domain.

On the other hand, the SWIFT affair has important repercussions for the EU's positioning as a global actor. A lively debate on the validity of understanding the EU's global role in terms of a normative power is taking place (Manners, 2002; Diez, 2005).

[2] Remarks by Vice-President Joe Biden to the European Parliament, Brussels, 6 May 2010. Available at: «http://www.whitehouse.gov/the-press-office/remarks-vice-president-biden-european-parliament».

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

This article argues that the resolution of the SWIFT affair tried to support and solidify the position of the EU as a global actor with normative appeal. However, the expected creation of a *European* Terrorism Financing Tracking System, coupled with the way in which the EU itself is keenly implementing risk-based and data-led (internal) security measures, means that one has to remain critical toward Europe's normative appeal, for it may, as Thomas Diez (2005, p. 627) has observed, 'allow EU actors to disregard their own shortcomings'.

I. New Institutional Configurations

The SWIFT affair has so far received surprisingly little attention in academic debate. Important analytical work is being done by legal scholar Paul de Hert and his colleagues around the implications of the affair on the legal regimes of privacy and data protection in the EU (De Hert and De Schutter, 2008; González Fuster *et al*., 2008). The SWIFT affair relates to, but has yet to receive attention within, the wider literature on new internal/external security initiatives developing at EU level in the context of the post-9/11 global order (for example, Edwards and Meyer, 2008; Bickerton *et al*., 2011). In particular, the SWIFT programme was rendered possible in the context of a set of novel and controversial security measures that acquired political urgency in the post-9/11 era, including new risk-based border controls, advanced European police and justice co-operation and terrorism asset freezing (Den Boer and Monar, 2002; Bigo and Tsoukala, 2008; Amoore and De Goede, 2008). The pursuit of the financing of terrorism, in which the Paris-based Financial Action Task Force (FATF) plays a key role, has become an important element of the post-9/11 security landscape, which, as I argue elsewhere, serves primarily to broaden and expand the domain of possible security intervention (De Goede, forthcoming).[3]

As briefly noted above, although the TFTP was initiated in October 2001, it was not publicly known until disclosed by the *New York Times* in June 2006. The newspaper revealed that the American Treasury and the CIA had sought and gained access to financial transactions data held by the private, Belgian-based company SWIFT, which handles about 80 per cent of all global wire transfer traffic. This was possible because SWIFT maintained a data processing centre based in the United States, where copies of all transactions were stored for 124 days. The Treasury issued subpoenas to SWIFT's processing centre, thus gaining access to the global data, including but not limited to those of American and European citizens. The Belgian Privacy Commission has established that the data were subpoenaed on the basis of broadly defined categories (for example, all transactions to and from country x between specific dates), and that the total transfer of data to the Treasury must have involved millions of records (Belgian Privacy Commission, 2006, pp. 3, 5).

Upon public disclosure of the existence of the TFTP, political debates in the United States took quite a different shape than those in the EU. This is important because the ways in which the TFTP was politicized was decisive for its institutional effects (Edkins, 1999; Debrix and Weber, 2003). In other words, the direction that controversy and debate took after the revelation of the TFTP was not pre-given, but depended upon contingent

[3] On the fight against terrorism financing, see also Levi and Wall (2004); Levi (2010); Biersteker and Eckert (2007); Warde (2007); Vlcek (2008).

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

processes of politicization in which existing notions of security, privacy and liberty were deployed to accord meaning and raise questions about this programme. In the United States, what quickly became controversial was the decision of the *New York Times* and the *Los Angeles Times* to proceed with publication of the story. Security officials pleaded with the papers not to publish, and condemned them for compromising national security when they did so (Stolberg and Lichtblau, 2006; Snow, 2006). The ensuing debate on national security, free speech and the responsibility of the press largely drowned out questions on the programme's implications for privacy and civil liberties.

In Europe, the TFTP was headline news after the revelation by the *New York Times*, and the core of the controversy became the way in which American security services had secretly accessed the private financial data of European citizens within United States jurisdiction and apparently without juridical oversight. Another contentious issue was the extent of the complicity of the SWIFT company, which had not contested the American subpoenas and had allowed access to its database, seemingly without regard for European privacy law. Jean-Marie Cavada of the European Liberals and Democrats called the matter a 'scandal' in the plenary meeting of the EP on 5 July 2006, and noted a clear breach of European law.[4]

In September 2006, the first opinion of the Belgian Privacy Commission (2006, pp. 5, 20) was released, which objected to the 'carpet sweeping' techniques deployed in the transfer of SWIFT data to the American authorities, and provisionally concluded that the programme entailed a 'secret, systematic, massive and enduring breach of the fundamental European principles concerning data protection'.[5] The Belgian Privacy Commission reproached SWIFT and demanded its compliance with European privacy law. This finding was broadly confirmed by the report of the EU's privacy watchdog Working Party 29 (WP29), which concluded in November 2006 that the data transfer procedure from SWIFT to the United States Treasury entailed a 'lack of transparency and adequate and effective control mechanisms', representing 'a serious breach' of the EU Data Protection Directive.[6]

Framed as an issue squarely concerned with privacy and data protection, and as one in which 'European values' were at stake, European Parliamentarians and (supra)national privacy bodies manifested themselves strongly in this debate, generating conflict between not just the EU and the United States, but also *within* the EU itself. This conflict involved more than the complex processes of decision-making that generally typify the EU, but entailed a fundamental struggle for authority concerning issues that cut across what used to be called the 'first and third pillars' amidst the shifting legal landscape of the Lisbon Treaty coming into force (cf. Niemann, 2006).

The internal EU politics in relation to the SWIFT affair revolved around two interlocking dynamics: first, there was the question of institutional competence and the issue

[4] EP hearings, 5 July 2006. Available at: «http://www.europarl.europa.eu/wps-europarl-internet/frd/vod/player?date=20060705&language=en, at 17"38'».

[5] 'een geheime, systematische, massale and jarenlange inbreuk op de fundamentele Europese beginselen inzake gegevensbescherming' (my translation).

[6] WP29, *Press Release on the SWIFT Case*, 23 November. Available at: «http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_23_11_06_en.pdf=». See also WP29, *Opinion 10/2006 on the Processing of Personal Data by SWIFT*, 22 November 2006. Available at: «http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf=». In February 2007, the European Data Protection Supervisor (EDPS) released an opinion dealing specifically with the role the European Central Bank (ECB) played in the affair.

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

of whether the SWIFT data properly belonged in the domain of commerce (first pillar) or internal security (third pillar). While couched in institutional language, the core question here was one of *accountability*: first-pillar competence set into motion different kinds of decisional dialogues and privacy protections than did third-pillar competence. The second dynamic revolved around the axis of public–private co-operation in EU governance, and the important role that the SWIFT company *itself* played in shaping the EU–US agreements on this issue and, indeed, the wider European privacy architecture.

These interlocking dynamics required not simply the elucidation of predefined areas of competence, but entailed more precisely a complex staking out of authority over the novel processes whereby commercial data are deployed for security practices. Thus, the politicization of the problem and the concomitant claims over institutional competence were not simply discursive framings, but rather sought to be *performative* – that is, they tried to establish (or, in the case of the European Central Bank, to disclaim) the authority to make decisions concerning the handling of the SWIFT data and transatlantic data exchange more generally (Butler, 1997; Bialasiewicz *et al*., 2007). Put simply, institutional competence did not pre-exist the legal and political struggle examined here, but the authority was claimed, contested and reclaimed over the course of the playing out of the SWIFT affair. Precisely because of the dissolution of the pillar structure, the EP had to develop and test its security competence in practice, and this is exactly what it did in relation to the SWIFT case. Perhaps even more than a success for European privacy law, then, the February 2010 vote that rejected the interim agreement involved an assertion of the EP's new powers under the Lisbon Treaty. In this context, EP chair Rouček Libor called the outcome of the vote a 'truly historic moment'.[7]

The first dynamic through which the SWIFT affair played out, then, concerns institutional competence and concomitant questions of accountability. From the moment of the disclosure of the TFTP in June 2006, the EP worked hard to claim competence over the issue and to shape the political discussions and decisions. In July, it adopted a resolution demanding clarification to what extent the European Commission and Council had been aware of the TFTP, and emphasizing the role of the European Central Bank (ECB) with regard to the protection of European citizens' financial data. The resolution voices strong disapproval of 'any secret operations [. . .] that affect the privacy of EU citizens' and deep concern over the fact that 'such operations should be taking place without the citizens of Europe and their parliamentary representation having been informed'.[8]

This resolution led to two Hearings in the EP, in October 2006 and March 2007, where the different parties to the SWIFT affair were invited to explain themselves – including the ECB and SWIFT – and where the issue was twinned with concerns over the transatlantic data-mining of Passenger Name Records (PNR). During these Hearings, representatives of the EP's Committee on Civil Liberties, Justice and Home Affairs, as well as experts in privacy law, delivered strong condemnations of the TFTP and its violations of privacy protection. They emphasized that any transfer of private data to security authorities

[7] See Note 1 above, at 12:22:12.

[8] Joint Motion for a Resolution, 5 July 2006. Available at: «http://www.europarl.europa.eu/sides/getDoc.do;jsessionid=BAD0D59097521F21D81BE04CBEBF1B61.node1?language=EN&type=MOTION&reference=P6-RC-2006-0386». See also *Euractiv* article at «http://www.euractiv.com/en/security/parliament-wants-information-SWIFT-cia-data-transfer/article-156625».

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

requires prior juridical authorization and should respect the rules of proportionality.[9] For example, Stefano Rodotà, Professor of Law and former Chairman of WP29, lamented the downward pressures placed on data protection because of 'internal and international security requirements [and] market interests'. He warned against a 'society based on surveillance, classification and social [. . .] sorting', and advocated the strengthening and globalization of a *European model* in which data protection is recognized as an autonomous right.[10]

For all its important activity in keeping the SWIFT affair on the political agendas, however, the EP initially had little success in claiming authority over this issue. The question concerning institutional competence revolved around the status of commercial data collected in the course of first-pillar activities (such as air travel or banking) which are redeployed for third-pillar purposes (policing and internal security). In his initial reaction before the EP in July 2006, Commission Vice-President Franco Frattini called this a 'grey area'. Importantly, in Frattini's understanding, the main data transfer took place between two branches of the private company SWIFT (the Belgian and the American one), which means that he considered the data transfer to be of primary commercial nature. Consequently, Frattini stated that the first-pillar directive on privacy (EU Data Protection Directive 95/46/EC of 1995) 'is probably the one we should apply'.[11] However, Frattini's statement was in tension with his own spokesperson's assertion that the directive does *not* apply to data transfer for security purposes (referring to the transfer from SWIFT's American processing centre to the United States Treasury).[12] Subsequently, the EU Council and Commission developed and maintained the latter position – that is, that the SWIFT data transfer was a third-pillar issue, firmly in the domain of policing and home affairs, and therefore not within reach of the Data Protection Directive or the legislative competence of the EP.

Frattini's statement was not simply a mistake, but is revealing of the complex and contested legal landscape that is arising within and outside the EU around the deployment of commercial data for security purposes – as can be illustrated by two, seemingly opposing, verdicts by the European Court of Justice (ECJ).[13] In 2006, the legality of the agreements concluded (in 2004) between the EU and the United States on the processing of air passenger data (PNR) was contested by the EP, which sought an annulment on the basis that the privacy protections established in this agreement were insufficient and not founded on the appropriate legal bases (Brouwer and Guild, 2006). In its judgment of 30 May 2006, the ECJ granted the annulment and ruled that data processing 'as necessary for safeguarding public security and for law-enforcement purposes' does not fall under first-pillar competence and within jurisdiction of the data protection directive.[14] Despite the fact that the PNR data are collected in the course of commercial activity by private operators, its processing by the United States Customs and Border Protection Agency is 'quite different in nature', according to the Court, and, by implication, lifts it out of

[9] For example in the programme of October 2006 meeting, p. 6. Available at: «http://www.europarl.europa.eu/hearings/20061004/libe/programme_en.pdf».
[10] Rodota, presentation before the EP, 27 March 2007.
[11] EP hearings, 5 July 2006. See Note 4 above.
[12] See *Euractiv* article cited in Note 8 above.
[13] Interview, senior official, European Data Protection Supervisor's Office, Brussels, January 2010.
[14] ECJ, *Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04*, 30 May 2006, para. 57. See also press release at: «http://curia.europa.eu/en/actu/communiques/cp06/aff/cp060046en.pdf».

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

first-pillar competence.[15] This judgment was a setback for the EP: although it achieved the annulment of the EU–US deal on the transfer of PNR data that it had hoped for, it was simultaneously relieved of competence over the issue.

The European Court's decision on PNR can be contrasted with its verdict in the case contesting the legal basis of the EU Data Retention Directive in 2009. This directive, adopted under first-pillar provisions in 2006, requires Member States to oblige service providers to retain telecommunications data, including (mobile) telephone, email and Internet data, for a period between six months and two years for access by law enforcement.[16] The legal basis of the directive was contested by Ireland, which argued before the Court that the directive's principal objective is to 'facilitate the investigation, detection and prosecution of crime, including terrorism', and that it therefore does not belong to first-pillar competence.[17] Consequently, Ireland – a country whose economy is strongly dependent on the telecommunications industry – sought annulment of the directive. In its decision delivered in February 2009, however, the European Court ruled against Ireland and upheld the legal basis of the directive on the grounds that its primary objective was to harmonize data retention provisions across the EU with 'a direct impact on the functioning of the internal market'. The Court further argued that the directive governs only the activities of commercial service providers and does not regulate the transfer of, or access to, such data by policing forces.[18] Here, the Court's arguments seem to be in tension with its 2006 PNR decision where it did *not* regard the primary commercial nature of the data collection as a convincing argument to confirm first-pillar competence.

Indeed, the Court's decisions in the 2006 PNR case and the 2009 Data Retention case are reconcilable only if one imagines, as the Court seems to do, a clear distinction between an economic domain, where data are collected and stored in the course of daily commercial activity, and a security domain, where data can be transferred for processing and analysis in the context of law enforcement. However, in practice, such clear distinction is untenable, and research has demonstrated that the deployment of commercial data for security decision depends upon a complex mixing of public and private space, whereby commercial actors are increasingly authorized to process and analyze data with a view to enabling security decisions.

In the SWIFT case, complex arrangements have been made between public and private parties with regard to the selection, processing and analysis of data. American Treasury officials are not given complete access to SWIFT database, but sets of data are selected by SWIFT, 'black-boxed' and made accessible to the officials. Treasury searches continue to be supervised by security-cleared, SWIFT employees, called 'scrutineers', who have 'round-the-clock' and 'real-time' access to the justification for individual searches, and the power to query or block Treasury's searches.[19] The actual practices taking shape through the deployment of private data and commercial data-mining techniques for security decisions defy the imagination of separate domains of data collection for commerce, on

[15] See para. 57 of ECJ judgment cited in Note 14 above.
[16] Directive 2006/24/EC, 15 March 2006. Available at: «http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF». The data retained do not include the *content* of communication.
[17] ECJ, *Judgment of the Court of Justice in Case C-301/06*, 10 February 2009, §28.
[18] ECJ, Press Release, 'Judgment of the Court of Justice in Case C-301/06, 10 February 2009', p. 2.
[19] *Second Report on the Processing of EU-Originating Personal Data by the United States Treasury Department for Counter-Terrorism Purposes*, Terrorist Financing Tracking Programme, Judge J.-L. Bruguiere, January 2010, EU Classified, p. 4. See also Belgian Privacy Commission (2006, p. 7).

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

the one hand, and data analysis for security, on the other, but point to a much more complex interweaving of security and economy (for example, Favarel-Garrigues *et al*., 2008; Amoore, 2009; Amoore and Hall, 2009; Hall and Mendel, forthcoming).

II. Data-Led Security: Public–Private Security Assemblages

This brings us to the second dynamic at work in the transformation of European governance relating to the SWIFT affair, which is that of public–private co-operation and the key role that SWIFT *itself* played in shaping the institutional configurations and juridical arrangements that would eventually legitimate the TFTP. It is undeniable that SWIFT found itself in a difficult position when faced with the American subpoenas that demanded access to its data. The Belgian Privacy Commission's 2006 report implies that SWIFT could have chosen to contest the subpoenas in an American court, but it also acknowledges that the company had a substantial interest in complying with American authorities (Belgian Privacy Commission, 2006, pp. 6, 20). SWIFT's own position throughout the discussions in 2006 and 2007 tirelessly emphasized that the company 'did its utmost to protect the data of its customers' by obtaining from the United States Treasury 'unique protections and assurances' that limited the amount of data made available and the scope of the data analysis.[20] These assurances were initiated in 2004, after SWIFT's directors had grown increasingly worried about the scale and the duration of the programme, and included the encryption ('black-boxing') of data transferred to the Treasury, the limitation of data searches to cases related to terrorism or its financing, and the continuing oversight of searches by SWIFT representatives.[21]

Crucial to the governing effects of the SWIFT affair is that these assurances, negotiated on an ad hoc basis between the United States Treasury and the private company SWIFT, were slowly accepted as a legitimate juridical framework and, indeed, a model for future cases. In its initial 2006 report, the Belgian Privacy Commission noted the existence of the assurances but judged them to be insufficient in the face of a 'secret, systematic [and] massive' breach of European data protection principles.[22] Subsequently, however, the guarantees acquired by SWIFT became a key factor in the high-level EU–US negotiations between 2006 and 2010. The first agreement on the matter, reached in July 2007, announced 'rigorous controls and safeguards' governing the handling of the SWIFT data (Commission, 2007, C/166/18). These controls and safeguards consisted largely of the formalization of the assurances negotiated by SWIFT in 2004, including the black-boxing of data, the limitation to terrorism-related searches and arrangements for oversight by SWIFT representatives as well as an outside auditor (Commission, 2007, C/166/20–C/166/22).[23] New in this agreement were provisions on the retention period of data (maximum of five years for data *not* extracted from the black box) and the

[20] Francis Vanbever, 'SWIFT Reiterates Calls for EU–US Dialogue on Security and Data Privacy', statement before the EP, 4 October 2006. Available at: «http://www.SWIFT.com/about_SWIFT/legal/compliance/statements_on_compliance/eu_parliament_hearing_SWIFT_statement_and_press_release.page»

[21] Vanbever, statement (see Note 20 above); also Belgian Privacy Commission (2006, p. 7).

[22] 'geheime, systematische, massale en jarenlange inbreuk op de fundamentele Europese beginselen inzake gegevensbescherming' (Belgian Privacy Commission, 2006, p. 20, my translation).

[23] The fact that these representations were based on the earlier assurances negotiated by SWIFT is confirmed in Belgian Privacy Commission (2008, p. 78, para. 241).

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

appointment of an 'eminent European person' charged with oversight over the representations (Commission, 2007).

Perhaps even more remarkable than the influence the SWIFT company had on the shape of the EU–US agreement, is the turnaround by the Belgian Privacy Commission, which in a full report released in 2008 concluded that its earlier allegations that SWIFT had breached European privacy law were unfounded. This report re-evaluated the assurances negotiated between SWIFT and the United States Treasury from what it called 'a better knowledge position and in light of the later events and developments' (Belgian Privacy Commission, 2008, p. 78, my translation) and now judged them to be sufficient. The Commission found that SWIFT's actions were 'careful [and] conscientious' and provided an effective and secure limitation of the data processing. Indeed, the Privacy Commission held up SWIFT's conduct as an important future reference for similar situations and the development of European assistance mechanisms around this issue area (Belgian Privacy Commission, 2008, p. 79). The ad hoc solutions negotiated over the course of the SWIFT affair, then, became slowly legitimized and institutionalized in successive EU–US agreements. They have not just become permanent fixtures in security integration, but have also become regarded as a possible mould for future public–private security co-operation.

The changing configurations of EU governing in the case of the SWIFT affair can only be partly comprehended through existing notions of multi-level governance (Hooghe and Marks, 2001) or experimentalist governing (Sabel and Zeitlin, 2010). Both concepts capture important elements of the case, including the diffuseness of authority and the multipolar and institutionally competitive decision-making practice. Importantly, the notion of 'experimentalist governing' draws attention to the processes of the 'recursive redefinition of means and ends' through which participants learn 'what problem they are solving, and what solution they are seeking, through the very process of problem solving' (Sabel and Zeitlin, 2010, p. 11). In other words, political negotiation does not proceed from a shared understanding of the nature of the problem and the ends to be achieved, but consists precisely of the discursive contestations over, and definitions of, means and ends. In the SWIFT case, these took the form of a struggle over the (re)definitions of competence with regard to commercial data redeployed for security purposes, and a redefinition of the SWIFT assurances from inadequate to conscientious and even exemplary. However, the SWIFT case did not, as experimentalist governing would imply, depend upon a more or less ordered devolution of competence to local authorities, with public consultations and feedback loops that enable institutional learning (for example, Newman, 2010). On the contrary, the governing practices set in motion by the SWIFT case were far more contentious, unpredictable and contradictory. They were characterized by the important role played by the private company SWIFT *itself* in shaping the transatlantic agreement and the nascent privacy architecture of the third pillar, and the novel and ad hoc invention of the position of the 'eminent person' to oversee procedure – but whose reports remain officially classified. Here, it is perhaps better to speak of the emergence of a public–private security *assemblage* in which a range of agents 'interact, co-operate and compete' to produce new forms of security governing (Abrahamsen and Williams, 2009, p. 3). A key question that arises here is the possibility of accountability amid such complex and messy assemblages of governing.

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

III. Global Europe: Normative Power and a European TFTS

In addition to shedding light on the changing EU institutional configurations, the SWIFT affair also illuminates the position of Europe as a security actor and relations with the United States in particular. Indeed, here we may observe a significant collapse of the boundaries between internal and external relations as global security programmes lead to transformations in EU institutional balance, and as the EU's internal security governing reaches beyond its formal border to stimulate co-operation with third countries (Burgess, 2009; Lavenex and Wichmann, 2009; Lavenex, 2008). Contemporary debates about the global role of the EU are heavily influenced by notions of it as a 'civilian' or a 'normative' power in which economic clout and normative guidance, instead of military might, are understood to underpin it (for example, Manners, 2002, 2008; Maull, 2005; Bachmann and Sidaway, 2009). In Ian Manners' (2002, p. 240) well-known phrasing, normative power is the power to 'shape conceptions of the normal'. Though much contested (for example, Diez, 2005; Merlingen, 2007), the idea of 'normative power' has become a powerful conceptual lens through which Europe's global positioning is often understood. What insights does the analysis of the SWIFT case bring to bear on the lively discussion concerning Europe as a 'normative power'? On the one hand, the emphasis on privacy, data protection and the rule of law in the affair seems to support and solidify the EU's global positioning as a normative power. On the other hand, however, this normative positioning accords legitimacy and normalcy to questionable security programmes, such as the development of a *European* TFTP. This calls for a continued critical perspective on Europe's supposedly normative identity.

There are different ways of reading the effects of the SWIFT affair in the context of the normative power discussion. One such reading can be based on Javier Argomaniz's (2009) analysis of the PNR case, in which he argues that the EU behaved as a 'norm-taker' instead of a norm-maker. According to Argomaniz, the use of passenger booking data for security policy was advocated and enforced by the United States and was slowly internalized by the EU through a process of 'norm mirroring'. However, against this reading of the EU as a 'norm-taker', one could argue that it is precisely the process of negotiation and bargaining that confirms the normative power thesis and that supports the interpretation of the EU as a political 'counterweight' to American unilateralism (Bretherton and Vogler, 2006). Both in the PNR and in the SWIFT cases, as we have seen, the EP has raised profound questions concerning the legality of the use of commercial data by security services and the consequences for privacy and data protection. Such critical questioning, as well as the actual transformations in transatlantic data exchange effected through Parliament's interference, could be read as a confirmation of the role of Europe as a 'check and balance' against American unilateral power, based on Europe's adherence to the rule of law (Balibar, 2004, p. 214; also Habermas and Derrida, 2003).

Consequently, we may evaluate the normative power thesis by examining more closely the EP's actual influence on the EU–US agreement on financial data exchange, and the way in which it sought to solidify the EU's role as a security actor. The 2007 representations discussed in the previous section were not the end of the affair: amid the mounting controversies, SWIFT announced that it would restructure its company architecture to create a European and a transatlantic processing centre. This meant that American security services would no longer be able to use subpoenas to access data on European wire

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

transfers.[24] Consequently, the United States sought a new agreement with the EU in order to guarantee continued access to the European data after SWIFT's restructuring, and such (interim) agreement was concluded on 30 November 2009 – *one day* before the Lisbon Treaty came into force.

The EP protested fiercely against its sidelining in the EU–US negotiations – most notably when Dutch MEP Jeanine Hennis-Plasschaert won the EP vote rejecting the interim agreement in February 2010, as described in the introduction to this article. This vote was important because it allowed the Parliament a further role in shaping the new EU–US agreement on the processing and transfer of financial messaging data that was concluded on 24 June 2010. Between the 2007 Representations and the 2010 Agreement, the EP achieved the inclusion of new stipulations concerning the prohibition on data mining (Article 5), transparency toward data subjects (Article 14) and rights to rectification, accuracy and redress (Articles 16–18). Although it remains to be seen what effect these stipulations will be able to have in practice, the EP achieved inclusion of certain juridical safeguards and measures for citizen protection into the new agreement.

Perhaps the most important stipulation of the 2010 EU–US agreement, however, is Article 11 on the expected introduction of an equivalent EU Terrorism Financing Tracking Programme. At the time of writing, the European Commission has just released an outline of available options for the establishment of a European Terrorist Finance Tracking System (TFTS) in order 'to contribute significantly to efforts to cut off terrorists' access to funding and materials and follow their transactions' (Commission, 2011, p. 1).[25] By insisting that SWIFT data are not transferred in bulk to the United States, but are selected, extracted and decrypted on European territory and under the supervision of Europol, significant steps toward the further development of a European security community are being taken. One of the purposes of revising the terms of the TFTP agreement, for Hennis-Plasschaert, was for the EU to show itself to be a 'true counterpart and not counterweight to the US', and enhance its own capacity to examine and judge SWIFT data in the context of counterterrorism.[26] The Commission proposal for a TFTS recasts the tracking of terrorism financing in the EU from a (temporary) programme to a (durable) system, and raises the possibilities of *broadening* the new European TFTS to include other uses such as the combating of organized crime and money laundering, and to other data providers or financial message types (Commission, 2011, pp. 7–8).[27]

In this light, it is important to shift the terms of the debate away from the question of whether the EU *is* or *is not* a normative power in order to analyze normative power *itself* as a narrative with the ability to accord community and identity to the EU's nascent security role. Such rephrasing of inquiry builds on the work of a number of authors, including Bachmann and Sidaway (2009) and Diez (2005, p 626), who encourage

[24] The subpoenas on the American processing centre, which includes transatlantic data, remained in place. Thanks to an anonymous *JCMS* referee for clarifying this point. See 'SWIFT Board Approves Messaging Re-architecture', 4 October 2007. Available at: «http://www.swift.com/about_swift/legal/compliance/statements_on_compliance/swift_board_approves_messaging_re_architecture/index.page».

[25] It is important to note that the effectiveness of the TFTP remains disputed because details of cases are unavailable in the public domain (see Wesseling *et al*., forthcoming).

[26] Online interview, Hennis-Plasschaert, quote at 4:06. Available at: «http://www.europeesparlement.nl/view/nl/press-release/pr-2010/pr-2010-March/pr-2010-Mar-2.html;jsessionid=6E82112BC2318A7093425303B65FBFD6».

[27] Whether this broadening of the system will be implemented will depend on discussions between the Union and Member States in the months and years to come.

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

researchers to enquire into the question of 'what the use of the term "normative power" *does*' (emphasis added). This shift in discussion also moves analysis away from the formal structures of the *European Union* –implying focus on institutional balance and formal competences – toward considering the wider notion of *Europe*, and more precisely the question how myths of 'global Europa' help shape and constrain the positioning of the EU in a global order (Manners, 2010; Wintle, 2009). As James Rogers (2009, pp. 833–4) has recently argued, narratives of security are crucial in fostering and (re)structuring 'the European polity and its role and identity as an international actor' (cf. Campbell, 1992).

Thus understood, we can say that the normative power narrative, as it is linked to issues of law, privacy and data protection, has the ability to accord an identity to the nascent European security community. The contemporary European security identity is constituted *precisely* through this appeal to transnational risk practice coupled with normative safeguards and a 'European privacy model'. Such risk practices govern the 'interstitial spaces' of European jurisdictions, which, as Walters and Haahr (2005, p. 106) have argued, is crucial to the constitution of a coherent European territory. In this context, European actors have proven themselves keen believers in the value of financial and other public and private data in the post-9/11 security landscape and the need for security services to be able to store, retrieve and analyze large amounts of such data.

This turn to financial data analysis for security purposes cannot simply be interpreted as an instance of the EU as 'norm-taker'. Even if it is the case that the SWIFT and PNR affairs were caused by American-initiated security programmes, in other domains the EU itself has propagated the logic of deploying risk technologies and data analysis for security purposes that seek to identify and disrupt security threats at the earliest possible stage (De Goede, 2008; Den Boer and Van Buuren, forthcoming). This is most clearly visible in the domain of migration, where the EU is expanding both the reach and the purpose of its databases in the name of security (Broeders, 2007; Huysmans, 2006; Guild, 2008). Moreover, the EU Third Money Laundering Directive of 2007, which has been far less visible and controversial than the TFTP, goes perhaps even further in its requirements for banks and other financial institutions to mine, track and report suspicious financial activity to authorities. In fact, at the highest levels of the EU bureaucracy, the turn to data-mining for security purposes has become accepted as self-evident – or, as a senior EU counter-errorism official has put it in an interview:

> It's very simple, if you just wait [until] the bomb is put in a crowded place and blows up to start an investigation [you are too late]. How can you do that otherwise? You need to know a bit earlier if people are plotting, if they attended a Madrassah, a training camp, if they are buying false documents, if they are collecting money. [. . .] In itself having a [. . .] stolen mobile phone, having a false ID and buying fertiliser [. . .] is not that [. . .] important, it's a petty crime. But if it's part of a plot to blow up a railway station with 2000 people it becomes much more serious. So if you don't try to infiltrate, intercept, follow closely, people who act suspicious, who you believe are plotting something, you will not prevent the act to happen.[28]

The EU's insistence on the respect for privacy, data protection and rights of redress has the effect of legitimating and solidifying risk-based security practices precisely by prescribing procedures and frameworks in which they can take place. As the new

[28] Interview, senior EU counterterrorism official, Brussels, May 2009.

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

Commission document on the TFTS puts it: '[I]f an EU terrorist finance tracking system [. . .] is to be established, it should be established in the interest of providing security to EU citizens [. . .] [and] taking the specificity of the EU legal and administrative framework into consideration' (Commission, 2011, p. 4). The coupling of ambitious risk-based counterterrorism initiatives with an insistence on respecting the European privacy model and the rule of law simultaneously lends a (normative) identity to the European security community and solidifies these security practices which are often transnational in nature. In other words, the EU–US agreement legitimates and solidifies the SWIFT data-mining programme by transforming it from a secret and supposedly temporary initiative into a permanent security system governed by the rule of law and rights of redress.

Conclusions: Accountability in EU Security

The SWIFT affair is interesting not just on its own merits, but deserves attention because it provides a powerful lens onto contemporary transformations in the configurations of European governing, both internally and externally. The SWIFT affair demonstrated forcefully the institutional challenges produced by the deployment of private, commercial data for security policy, and the concomitant piecemeal, ad hoc innovations produced in governing practices. This article has shown how the struggle over competence over this issue entails a performative constitution of the EP's power over security matters as well as private involvement in shaping the nascent European privacy architecture regarding security measures. The article has further considered how the SWIFT affair has allowed the EU to position itself in the global security landscape as a normative power that promotes and adheres to *European* values of privacy and data protection. The transatlantic negotiations and the 2010 EU–US Agreement have a legitimating effect: they transformed and consolidated the TFTP from a secret and temporary measure to an enduring and rule-based transatlantic security programme. This fits into a broader practice of accessing and analyzing citizens' financial and commercial data in the name of pursuing terrorism and its financing.

Diez (2005) has argued that the narrative of normative power constructs the EU's identity in ways that may discourage critical self-reflection. The effects of narratives of normative power Europe may be to render invisible and indeed unquestioned the EU's *own* commitment to specific security programmes and their contestable normative implications. On the eve of the EU's own implementation of a Terrorism Financing Tracking Programme, therefore, it is important to reflect on the continuing problems of accountability that such a programme entails, even after the safeguards and restrictions imposed through successive rounds of negotiations. Accountability here cannot just be measured in terms of institutional feedback loops and learning, because – as we have seen – the process of by which the TFTP agreement was reached was largely ad hoc and fluid. Accountability, then, is used in a broad sense, involving transparency and justification toward the European citizenry (Bovens *et al*., 2010). The mechanisms for review and procedural safeguard that were achieved by the EP in its negotiations over the SWIFT affair still show substantial shortcomings. Thus, the 'eminent person' who oversaw the procedure whereby the data are transferred to the United States before 2010 was French judge Bruguières, known for his staunch support of data-led counterterrorism programmes in France for many years. Bruguières issued two

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

reports – which formally remain classified[29] – but these review only the procedures whereby the SWIFT data are transferred to the United States Treasury under continuing oversight of SWIFT employees. The same can (for the moment) be said about the role of Europol, which oversees the data transfers since the coming into force of the 2010 agreement, but which has been reproached by its supervisor for allowing American data requests that are very 'broad' and 'abstract' (Europol, 2011, p. 5). Neither Bruguières nor Europol has the competence or means to analyze the arguably much more important question of how financial data are selected, analyzed and made actionable.

It is precisely in relation to the analysis and actionability of financial data, however, that substantial critical questions can be asked which are not easily answered by the imposition of a 'European model' of privacy protection. Thus, one of Bruguières' leaked reports documents that TFTP searches are considered legitimate if there is a 'nexus' between the transaction and terrorism.[30] But what does such a 'nexus' involve? On what is it based, how broadly is it defined, and how can it be demonstrated and assessed? How can we guarantee that such a nexus to terrorism does not lead to the examination of the transactions of millions of citizens? More importantly, how does the 'nexus' between specific transactions and the suspicion of terrorism lead to specific security interventions, and how can we ensure that rules of evidence and the rights of suspects remain respected in such interventions? These are but some of the questions that need to be addressed urgently and openly if Europe is to live up to its normative power image.

Correspondence:
Marieke de Goede
Department of Politics
University of Amsterdam
OZ Achterburgwal 237
Amsterdam 1012DL
The Netherlands
email: m.degoede@uva.nl

References

Abrahamsen, R. and Williams, M.C. (2009) 'Security beyond the State: Global Security Assemblages in International Politics'. *International Political Sociology*, Vol. 3, No. 1, pp. 1–17.

Amicelle, A. (2011) 'The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the "SWIFT Affair" '. *Research Question 36* (Paris: Centre d'études et de recherches internationals, Sciences Po). Available at: «http://www.ceri-sciences-po.org/publica/question/qdr36.pdf».

Amoore, L. (2009) 'Algorithmic War: Everyday Geographies of the War on Terror'. *Antipode*, Vol. 41, No. 1, pp. 49–69.

Amoore, L. and De Goede, M. (2008) 'Transactions after 9/11: The Banal Face of the Preemptive Strike'. *Transactions of the Institute of British Geographers*, Vol. 33, No. 2, pp. 173–185.

Amoore, L. and Hall, A. (2009) 'Taking People Apart: Digitised Dissection and the Body at the Border'. *Environment and Planning D: Society and Space*, Vol. 27, No. 3, pp. 444–64.

Anderson, B. (2010) 'Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies'. *Progress in Human Geography*, Vol. 34, No. 6, pp. 777–98.

[29] One of Bruguières' reports has been leaked and is available online.
[30] See *Second Report*, Terrorist Financing Tracking Programme, cited in Note 19 above.

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

Aradau, C. and Van Munster, R. (2007) 'Governing Terrorism through Risk: Taking Precautions, (Un)knowing the Future'. *European Journal of International Relations*, Vol. 13, No. 1, pp. 89–115.

Argomaniz, J. (2009) 'The Passenger Name Records Agreement and the European Union Internalisation of US Border Security Norms'. *Journal of European Integration*, Vol. 31, No. 1, pp. 119–36.

Bachmann, V. and Sidaway, J.D. (2009) '*Zivilmacht Europa*: A Critical Geopolitics of the European Union as a Global Power'. *Transactions of the Institute of British Geographers*, Vol. 34, No. 1, pp. 94–109.

Balibar, É. (2004) *We the People of Europe?* (Princeton, NJ: Princeton University Press).

Belgian Privacy Commission (2006) *Advies nr 37*, 27 September (Brussels: Commissie voor de Bescherming van de Persoonlijke Levenssfeer).

Belgian Privacy Commission (2008) *Beslissing van 9 december 2008* (Brussels: Commissie voor de Bescherming van de Persoonlijke Levenssfeer). Available at: «http://www.privacycommission.be/nl/static/pdf/cbpl-documents/SWIFT-nl-final-09.pdf».

Bialasiewicz, L., Campbell, D., Elden, S., Graham, S., Jeffrey, A. and Williams, A. (2007) 'Performing Security: The Imaginative Geographies of Current US Strategy'. *Political Geography*, Vol. 26, No. 4, pp. 405–22.

Bickerton, C.J., Irondelle, B. and Menon, A. (2011) 'Security Cooperation beyond the Nation-State: The EU's Common Security and Defence Policy'. *JCMS*, Vol. 49, No. 1, pp. 1–21.

Biersteker, T.J. and Eckert, S.E. (eds) (2007a) *Countering the Financing of Terrorism* (London: Routledge).

Bigo, D. and Tsoukala, A. (eds) (2008) *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (London: Routledge).

Bovens, M., Curtin, D. and 't Hart, P. (2010) *The Real World of EU Accountability: What Deficit?* (Oxford: Oxford University Press).

Bretherton, C. and Vogler, J. (2006) *The European Union as a Global Actor* (London: Routledge).

Broeders, D. (2007) 'The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants'. *International Sociology*, Vol. 22, No. 1, pp. 71–92.

Brouwer, E. and Guild, E. (2006) 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US'. *CEPS Policy Brief 109* (Brussels: Centre for European Policy Studies).

Burgess, J.P. (2009) 'There is No European Security, Only European Securities'. *Cooperation and Conflict*, Vol. 44, No. 3, pp. 309–28.

Butler, J. (1997) *Excitable Speech: A Politics of the Performative* (New York: Routledge).

Campbell, D. (1992) *Writing Security: United States Foreign Policy and the Politics of Identity* (Minneapolis, MN: University of Minnesota Press).

Commission of the European Communities (2007) 'Processing of EU originating personal data by United States Treasury Department'. *Official Journal*, 20 July. Available at: «http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:166:0018:0025:EN:PDF».

Commission of the European Communities (2011) 'Communication from the Commission to the European Parliament and the Council: A European terrorist finance tracking system, available options'. *Brussels*, 13 July. Available at: «http://ec.europa.eu/home-affairs/news/intro/docs/110713/1_EN_ACT_part1_v15.pdf».

Council of the European Union (2010) 'Council decision on the conclusion of the agreement between the European Union and the USA on the processing and transfer of financial messaging data'. 2010/0178, Brussels, 24 June.

Debrix, F. and Weber, C. (eds) (2003) *Rituals of Mediation: International Politics and Social Meaning* (Minneapolis, MN: University of Minnesota Press).

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

De Goede, M. (2008) 'The Politics of Preemption and the War on Terror in Europe'. *European Journal of International Relations*, Vol. 14, No. 1, pp. 161–85.
De Goede, M. (forthcoming) *Speculative Security: The Politics of Pursuing Terrorist Monies* (Minneapolis, MN: University of Minnesota Press).
De Hert, P.J.A. and De Schutter, B. (2008). 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT'. In Thiel, S. and Martenczuk, B. (eds) *Justice, Liberty, Security: New Challenges for EU External Relations* (Brussels: VUB Press).
Den Boer, M. and Monar, J. (2002) '11 September and the Challenge of Global Terrorism to the EU as a Security Actor'. *JCMS*, Vol. 40, No. 3, pp. 11–28.
Den Boer, M. and Van Buuren, J. (forthcoming) 'Security Clouds: Towards an Ethical Governance of Surveillance in Europe'. *Journal of Cultural Economy*.
Diez, T. (2005) 'Constructing Self and Changing Others: Reconsidering "Normative Power Europe" '. *Millennium*, Vol. 33, No. 3, pp. 613–36.
Edkins, J. (1999) *Poststructuralism and International Relations: Bringing the Political Back In* (London: Lynne Rienner).
Edwards, G. and Meyer, C.O. (2008) 'Introduction: Charting a Contested Transformation'. *JCMS*, Vol. 46, No. 1, pp. 1–25.
Europol (2011) 'Joint Supervisory Body Report on the Inspection of Europol's Implementation of the TFTP Agreement'. Report JBS/Ins. 11-07. Brussels, 1 March. Available at: «http://europoljsb.consilium.europa.eu/media/111009/terrorist%20finance%20tracking%20program%20(tftp)%20inspection%20report%20-%20public%20version.pdf».
Favarel-Garrigues, G., Godefroy, T. and Lascoumes, P. (2008) 'Sentinels in the Banking Industry: Private Actors and the Fight against Money Laundering in France'. *British Journal of Sociology*, Vol. 48, No. 1, pp. 1–19.
González Fuster, G., De Hert, P. and Gutwirth, S. (2008) 'SWIFT and the Vulnerability of Transatlantic Data Transfers'. *International Review of Law, Computers and Technology*, Vol. 22, No. 1, pp. 191–202.
Guild, E. (2008) 'The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the "Terrorist Lists" '. *JCMS*, Vol. 46, No. 1, pp. 173–93.
Habermas, J. and Derrida, J. (2003) 'A Plea for a Common Foreign Policy, Beginning in the Core of Europe'. *Constellations*, Vol. 10, No. 3, pp. 291–97.
Hall, A. and Mendel, J. (forthcoming) 'Threatprints, Threads and Triggers'. *Journal of Cultural Economy*.
Hooghe, L. and Marks, G. (2001) *Multilevel Governance and European Integration* (Lanham, MD: Rowman & Littlefield).
Huysmans, J. (2006) *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (London: Routledge).
Lavenex, S. (2008) 'A Governance Perspective on European Neighborhood Policy: Integration Beyond Conditionality?' *Journal of European Public Policy*, Vol. 15, pp. 938–55.
Lavenex, S. and Wichmann, N. (2009) 'The External Governance of EU Internal Security'. *Journal of European Integration*, Vol. 31, No. 1, pp. 83–102.
Levi, M. (2010) 'Combating the Financing of Terrorism: A History and Assessment of the Control of "Threat Finance" '. *British Journal of Criminology*, Vol. 50, No. 4, pp. 650–96.
Levi, M. and Wall, D.S. (2004) 'Technologies, Security and Privacy in the Post-9/11 European Information Society'. *Journal of Law and Society*, Vol. 31, No. 2, pp. 194–220.
Lichtblau, E. and Risen, J. (2006) 'Bank Data is Sifted by US in Secret to Block Terror'. *New York Times*, 23 June.
Manners, I. (2002) 'Normative Power Europe: A Contradiction in Terms'. *JCMS*, Vol. 40, No. 2, pp. 235–58.

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd

Manners, I. (2008) 'The Normative Ethics of the European Union'. *International Affairs*, Vol. 84, No. 1, pp. 45–60.
Manners, I. (2010) 'Global Europa: Mythology of the European Union in World Politics'. *JCMS*, Vol. 48, No. 1, pp. 67–87.
Maull, H.W. (2005) 'Europe and the New Balance of Global Order'. *International Affairs*, Vol. 81, No. 4, pp. 775–99.
Merlingen, M. (2007) 'Everything is Dangerous: A Critique of Normative Power Europe'. *Security Dialogue*, Vol. 38, No. 4, pp. 435–53.
Newman, A. (2010) 'Innovating European Data Privacy Regulation: Unintended Pathways and Experimentalist Governance'. In Sabel, C. and Zeitlin, J. (eds) *Experimentalist Governance in the European Union: Towards a New Architecture* (Oxford: Oxford University Press).
Niemann, A. (2006) *Explaining Decisions in the European Union* (Cambridge: Cambridge University Press).
Rogers, J. (2009) 'From Civilian Power to Global Power: Explicating the European Union's Grand Strategy through the Articulation of Discourse Theory'. *JCMS*, Vol. 47, No. 4, pp. 831–62.
Sabel, C. and Zeitlin, J. (eds) (2010) *Experimentalist Governance in the European Union: Towards a New Architecture* (Oxford: Oxford University Press).
Snow, J. (2006) 'Letter to the Editors of the *New York Times* by Treasury Secretary Snow'. *New York Times*, 26 June.
Stolberg, S.G. and Lichtblau, E. (2006) 'Cheney Assails Press on Report on Bank Data'. *New York Times*, 24 June.
Vlcek, W. (2008) 'A Leviathan Rejuvenated: Surveillance, Money Laundering and the War on Terror'. *International Journal of Politics, Culture and Society*, Vol. 20, No. 1–4, pp. 21–40.
Walters, W. and Haahr, J.-H. (2005) *Governing Europe: Discourse, Governmentality and European Integration* (London: Routledge).
Warde, I. (2007) *The Price of Fear: Al-Qaeda and the Truth Behind the Financial War on Terror* (London: I.B. Taurus).
Wesseling, M., De Goede, M. and Amoore, L. (forthcoming) 'Datawars beyond Surveillance: Opening the Black Box of SWIFT'. *Journal of Cultural Economy*.
Wintle, M. (2009) *The Image of Europe* (Cambridge: Cambridge University Press).

© 2011 The Author(s) JCMS: Journal of Common Market Studies © 2011 Blackwell Publishing Ltd