AICGS ISSUEBRIEF

MAY 2010 35

Anything but SWIFT: Why Data Sharing is Still a Problem for the EU

BY EDNA DRETZKA AND STORMY-ANNIKA MILDNER

Why has the European Parliament rejected the interim agreement on sharing banking data with the U.S.?

What are U.S. and EU approaches to data protection? In how far do privacy concerns and laws differ?

What are potential solutions to the SWIFT dispute?

"I want to counter the impression that the door now is wide open for terrorism. That is simply not true. It is still quite possible to get information in targeted questions. […] I am happy how after Lisbon the coordinates are shifting in favor of Europe" (German Minister of Justice, Sabine Leutheusser-Schnarrenberger after the EU Parliament voted down an agreement on sharing banking data with the U.S.).[1]

"The U.S. Administration may have wrongly thought they could deal with the European Parliament like Gulliver with the Lilliputians. Under the Swedish Presidency, European governments and the Council also made a mistake to believe it would be possible to force the European Parliament to give its consent on an unacceptable agreement based more on the U.S. approach to security than on the EU's defense of citizens' fundamental rights" (Socialists and Democrats group leader in the European Parliament Martin Schulz).[2]

"If [SWIFT] were to fail, it would be very, very damaging. [Europe, and Germany in particular, are currently] being targeted by Islamic terrorism and, thus, are the main beneficiaries of SWIFT reports" (Adam Szubin, Director of the Treasury's Office of Foreign Assets Control, in charge of the Terrorist Finance Tracking Program).[3]

In early February 2010, the European Parliament rejected an interim agreement between the European Union and the United States on sharing banking data, which would have given the U.S. continued access to data compiled by SWIFT (Society for Worldwide Interbank Financial Telecommunications), a private company set up in 1973 for the exchange of financial messages between institutions. With the vote against the agreement, the Parliament wanted to demonstrate its commitment to protect its citizens from the abuse of power by members of the European Council and also from the United States bullying Europe into unfavorable transatlantic agreements. According to European Parliament President Jerzy Buzek, the correct balance between security on the one hand and the protection of civil liberties and fundamental rights on the other was not reflected in the interim agreement given by the Council to the Parliament.[4]

The issue of data protection and privacy is contentious within EU-U.S. cooperation. Controversies range from the transfer of passenger name records (PNR) data to the U.S. Customs and Border Protection to the use of SWIFT data for the fight against terrorism—many of these still remain to be solved.[5] The U.S. sees the SWIFT agreement as "the first major test of trans-Atlantic cooperation on security post-Lisbon Treaty."[6]

Introduction

After the September 11, 2001 (9/11) terrorist attacks in New York City, the United States government and its allies went into red alert, implementing new instruments to track down terrorists. One such instrument, used to find and cut off terrorist funding, is the Terrorist Finance Tracking Program (TFTP). It monitors financial transaction data of suspected terrorists. After U.S. intelligence sources identify an individual or entity, the Treasury department subpoenas a "limited subset of data"[7] from the international banking network known as SWIFT. SWIFT data is then used to map out and prevent the funding of terrorist networks. In order to keep the element of surprise when pursuing suspects, the U.S. government initially kept this program a secret from European governments. As a result, when the *New York Times*, the *Wall Street Journal*, and other news sources[8] published articles exposing the program in June 2006, it incited the anger of several European governments. While the U.S. House of Representatives passed HR 895, voicing support for the Treasury Terrorist Finance Tracking Program as lawful and condemning the unauthorized disclosure of classified information by the media, the European Parliament demanded that a framework be established to ensure appropriate data protection and prevent the data from being used for purposes other than counterterrorism. The EU and U.S. then set up a transatlantic dialogue to obtain certain safeguards. In addition, the European Commission tasked Judge Jean-Louis Bruguière with analyzing whether or not the United States had given guarantees on the protection of personal data.[9] It was not until mid-2009, however, that the U.S. was forced to change its practices, after SWIFT had moved parts of its servers from the U.S. to Europe—intra-European data was now stored only in Europe; until then the data had also been kept on a server in the United States—taking away the subpoena rights[10] that the U.S. had on its own soil.

The future of TFTP as the U.S. knows it depends on whether or not it can strike a data-sharing deal with the European Union, one that is blessed by the European Parliament. An agreement is needed because European data protection laws prohibit the passing of personal data to the U.S. It appears that the U.S. must fight an uphill battle not only to convince Europeans of the necessity and legality of the program, especially in light of the treasured idea of *Datenschutz* (personal data protection), but that the U.S. will also have to deal with the political in-fighting between the Council and the European Parliament.

The U.S. Story: Legal Underpinnings

According to the U.S. Treasury Department, the SWIFT program is supported by both domestic and international laws: Domestically, "the TFTP is firmly rooted in sound legal authority, based on statutory mandates and Executive Orders."[11] This includes the United Nations Participation Act of 1945 (UNPA) and the International Emergency Economic Powers Act of 1977 (IEEPA). Both laws were passed by the U.S. Congress, extending power to the President to sanction countries or nationals in response to unusual, extraordinary threats to national security. President George W. Bush found that the terrorist acts of 9/11 constituted just such an extraordinary threat, thereby declaring a national emergency. He then issued Executive Order 13224, invoking broad powers under the IEEPA to authorize the Treasury Office of Foreign Asset Control (OFAC) to administer sanction programs against named individuals and entities, as designated by the Secretaries of State, Treasury, and the Attorney General. These government entities are empowered to "investigate, regulate, or prohibit (i) any transactions in foreign exchange, (ii) transfers of credit or payments between, by, through, or to any banking institution, to the extent that such transfers or payments involve any interest of any foreign country or a national thereof, (iii) the importing or exporting of currency or securities, by any person, or with respect to any property, subject to the jurisdiction of the United States."[12] In addition, the IEEPA was interpreted to authorize the government to require reports of transactions and to subpoena "[…] the production of any books of account, records, contracts, letters, memoranda, or other papers"[13] relating to any matter under investigation.[14]

WHAT IS SWIFT

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) was founded in 1973 as a member-owned cooperative organization between financial institutions around the world, in order to facilitate electronic financial transactions through a safe and efficient transfer of information. It does not hold funds nor does it perform account management services. It is a communication platform between its members, through which millions of standardized financial messages are passed daily. It also serves as a discussion forum that helps the worldwide financial community work together to establish market practice, set standards, and consider solutions. SWIFT handles about 80 percent of all international financial transactions from some 208 countries.

Internally, SWIFT is structured like most public companies. Its shareholders elect a Board of 25 Independent Directors, which is responsible for government and management oversight of the company. With over 8,300 banking organizations, securities institutions, and corporate customers in over 208 countries using SWIFT services, the Cooperative recognizes that the Central Banks in each of its member countries have a duty to foster financial stability. It has therefore agreed to cooperative oversight by the central banks of the Group of Ten Countries (G-10), coordinated by the National Bank of Belgium (NBB). The NBB has a written agreement with the other financial overseers that lays down the oversight objectives, and it acts on their behalf when it periodically reviews SWIFT's procedures of identification and mitigation of operational risks, legal risks, transparency of arrangements, and customer access policies.

According to SWIFT, its Board of Directors and its oversight committee, made up of all of the G-10 countries, were aware of the U.S. government's subpoenas, although it did express concerns about the legality of the operation. According to the *The New York Times*, the SWIFT executives told American officials they were considering pulling out of the arrangement by 2003. Worried about potential legal liability, the SWIFT executives agreed to continue providing the data only after top officials, including Alan Greenspan, then chairman of the Federal Reserve, intervened. Since that time, SWIFT has worked with the Belgian Data Commission, the European Union, and its members to demonstrate legal compliance. These efforts culminated in 2009, when SWIFT moved its European data servers to European soil, thus making it subject to European governments' laws, not the United States' regulations.

PRIVACY PROTECTION IN THE UNITED STATES

In contrast to the EU, which centrally supervises the private sector's use of personal data, the U.S. has, to date, no single, comprehensive data protection legislation. Instead, a sectoral approach is followed, with a mix of legislation, regulation, and self-regulation. Rules are specific and narrowly applicable. While European privacy legislation defines a set of principles for the treatment of personal data without regard to whether the data is held in the public or private sector, in the United States the legal tradition is much more concerned with regulating data collected by the federal government. Data protection in the private sector is largely self-regulatory. One explanation for the U.S. approach could be a stronger faith in the markets as well as in the court system, based on the long case history in the Supreme Court in deciding matters of data security.

Privacy rights in the U.S. can be divided into two categories: those under common law and those regulated by the government. The discussion of privacy rights in the U.S. extends back as far as 1890 with an article in the Harvard Law Review called "The Right to Privacy." Its authors, Samuel D. Warren and Louis D. Brandeis, were concerned with disclosing and publicizing personal information, especially by the press. Warren and Brandeis defined privacy right as "the right to be let alone." In 1960, legal scholar William Prosser discussed the current state of privacy in tort law. He identified four aspects of privacy breaches: Intrusion upon seclusion or solitude, or into private affairs; public disclosure of embarrassing private facts; publicity which places a person in a false light in the public eye; and appropriation of name or likeness.

The right to privacy is not guaranteed *per se* by the U.S. Constitution—the term "privacy" does not appear in the Constitution or the Bill of Rights—although the Supreme Court has ruled that privacy is protected through a combination of other rules and regulations. At the federal level, the Bill of Rights protects the right to Freedom of Speech (1st Amendment), Protection of Unreasonable Search and Seizure (4th Amendment), and the Due Process Clause (5th Amendment, protection against abuse of government authority in a legal procedure). The 14th Amendment includes a similar Due Process Clause, except that it is used to apply most of the Bill of Rights to the states. Many states have set up their own Office of Privacy or Office of Information to protect these rights. Nevertheless, these laws protect individuals, not their personal information specifically.

More specific protection of personal data is provided, for example, by the Right to Privacy Act of 1974 and the Right to Financial Privacy Act of 1978. The 1974 law regulates the intrusion of state actors into citizens' private lives by requiring consent from an individual to release his/her private information, except under one of twelve statutory exemptions. Government agencies must have a security system in place to protect the data as well as a Data Integrity Board. The Right to Financial Privacy Act of 1978 was a response to a Supreme Court decision, which found that bank customers had no legal right to privacy for their information held by financial institutions. Both of these laws are largely procedural, requiring government agencies to provide notice and an opportunity to object before forcing financial institutions to release personal financial information.

For further reading see for example: Avner Levin and Mary Jo Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground," University of Ottawa Law & Technology Journal, Vol. 2, No. 2, 2005: 357-395.

Other U.S. laws that were interpreted to apply toward the SWIFT program included Title III of the U.S. Patriot Act of 2001 and the Intelligence Reform and Terrorism Prevention Act of 2004. These were domestic laws aimed at the government's access to financial institutions' records in order to determine if there was evidence of money laundering, counterfeiting, or other illegal transactions taking place within the U.S. or using a foreign bank with an interbank account in a U.S. institution. While the U.S. Right to Financial Privacy Act of 1978 would have restricted government access to Americans' banking records in financial institutions, in this case SWIFT was considered a messaging service and was thus exempt from the law governing privacy.

Internationally, the U.S. claimed compliance with the UN Charter through the UNPA and the Belgian Data Protection Commission. The UNPA was passed by Congress to accompany the U.S. ratification of the UN Charter in 1945 and was intended to "prescribe the domestic, internal arrangements within [the U.S.] Government for giving effect to [U.S.] participation in [the United Nations] and [to] set up the machinery whereby [U.S.] national authorities can comply with certain of the major international commitments."[15] Compliance with UNPA, as amended (22 U.S.C. 287c) (UNPA), means that the U.S. must implement measures previously ordered by the UN Security Council in response to a Security Council mandate. After 9/11, President Bush invoked the UNPA in response to two Security Council Resolutions: 1368 (2001) on 12 September 2001 and 1373 (2001) on 28 September 2001[16] and also in response to the UN International Convention for the Suppression and Financing of Terrorism of 1999. This last measure was adopted by the UN General Assembly and required UN member states to "take measures to identify, discover, freeze, or seize the moneys used or intended for use to finance terrorist attacks of an international character."[17]

According to the Congressional Research Service's assessment, the UNPA "appears to cover the types of monitoring at issue, at least so long as the measures are calibrated to monitor only transactions that are reasonably related to an investigation of possible terrorist financing and are otherwise constitutional."[18] U.S. representations to the UN Council confirmed that financial transaction record information was limited in scope and calibrated appropriately. Information requests were limited to the originator and recipient of the transaction, including name, account number, address, national identification number, and other personal data, but did not include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health data.[19]

After the initial disclosure of the program in June 2006, the SWIFT program found support from the Belgian Data Protection Commission and from a European-appointed expert analyzing the program (Bruguière report). In November 2006, six months after the program was exposed, an EU-U.S. Justice and Home Affairs Ministerial was set up to establish common principles on outstanding issues relating to privacy and personal data protection, especially with regard to the European Data Protection Directive (Directive 95/46/EC).[20] In June 2007, an agreement between the U.S. and EU established the program's parameters and entered into a series of commitments, as negotiated by the Council and the European Commission.[21]

As part of the June 2007 agreement, the European Commission named Judge Jean-Louis Bruguière as the so-called "eminent" European person in charge of verifying U.S. compliance with the TFTP Representations. Judge Bruguière produced two reports, one

in December 2008 and the second in February 2010, both underscoring the significant value of the TFTP in the investigation and disruption of terrorism.[22] SWIFT also received international justification regarding its actions when, after a two year study, the Belgian Data Protection Commission concluded on 9 December 2008 that SWIFT complied with all applicable Belgian legislation.[23]

The U.S. argues that it has been compliant and vigilant of people's rights, while performing a public service both abroad and at home. According to Stuart Levey, Undersecretary for Terrorism and Financial Intelligence, U.S. Treasury Department, the TFTP provided more than 1,500 reports and countless leads to counterterrorism investigators in Europe and more to other countries. This included information provided during the investigation of the foiled 2006 Al-Qaeda plot to attack transatlantic flights between Europe and the U.S.

Political Wrangling: Council vs. Parliament and Different Priorities

From 2006 through 2009, there was a unified European response to the SWIFT program through the Council. On 29 June 2007, the German EU Council presidency and the European Commission welcomed the agreement reached on the transfer to U.S. authorities of data gathered by SWIFT.[24] Nevertheless, just two and a half years later, attempts to temporarily extend this agreement for nine months until a more permanent solution was drafted were scuttled.

The catalyst for this development was two-fold: the "dual-zone program" instituted by SWIFT and the implementation of the Lisbon Treaty on the European Union. Despite standing by its assertion that the data subpoenaed by the U.S. Treasury for anti-terrorism purposes was limited, protected, targeted, independently audited, and monitored,[25] SWIFT created two zones of data by moving European transaction data off U.S. soil and out of the reach of U.S. subpoena power. This was done to allay SWIFT's clients' privacy concerns. SWIFT's move to the dual-zone system moved the onus off the company and onto the countries to negotiate the politics of the situation.

Thus, when the first stage of the relocation program was activated in August 2009,[26] the U.S. needed an agreement with the EU to use the data. In order to keep continuity within TFTP while working out a longer term agreement between the EU and the U.S. on data sharing, the Council negotiated a temporary agreement in November 2009 to allow the U.S. to continue accessing SWIFT data for security purposes until August 2010. In a resolution adopted on 17 September 2009, the European Parliament said that data should be gathered "only for the purpose of fighting terrorism" and "the right balance" must be kept between security measures and the protection of civil liberties.[27] Members of the European Parliament (MEPs) were particularly critical of the fact that the agreement allowed transfers of data not only relating to specific suspects, but also "in bulk": If SWIFT was unable to produce specific data for technical reasons, it would provide "all potentially relevant data in bulk" to U.S. authorities instead. Jeanine Hennis-Plasschaert, rapporteur on the issue in Parliament, argued "with the proposed interim-agreement we instead rely on broad administrative subpoenas for millions of records of European citizens. By the very nature of SWIFT it is not possible to refer to so-called limited requests. For technical and governance reasons SWIFT has to transfer bulk data, thereby violating the basic principles of EU data protection law such as necessity and proportionality. And this cannot be rectified *ex-post* by mechanisms of oversight and control."[28] Most notably the liberal faction in the Parliament repeatedly criticized the agreement as "not only a restraint on European sovereignty but a massive intrusion into every single European citizen's privacy."[29]

Two months later, in November 2009, the Council, perhaps sensing resistance from the Parliament, voted in favor of extending the agreement until August 2010. Indeed, Parliament overturned this decision in February 2010. Because of concerns about information and security gaps, the European Parliament vetoed the interim agreement with a 378-196 vote, plus 31 abstentions, underscoring political and ideological differences within the Union. MEPs called on the Commission and Council to start work on a long-term agreement with the U.S. on this matter, arguing that any new accord had to meet the criteria of the Lisbon Treaty, and in particular comply with the Charter of Fundamental Rights.[30]

The question arises, what happened in the intervening time between 2007 and 2010 that eroded European support of the SWIFT program. Politically, the SWIFT issue has become grounds for a power struggle between the Council and the European Parliament, the bicameral arms of the European Union's legislature. Ideologically, the vote exposed the differences in the scope of individuals' data protection rights as seen by different members of the EU. Member states in the Council voted for the trumping of national security interests over individual data security, whereas the representatives of EU citizens in Parliament voted in the opposite direction. A division along these lines is not unsurprising, given the constituencies of each of these legislatures. The Council is made up of representatives of the national governments in the EU with a history of voting in favor of the SWIFT program, whereas Parliament is popularly elected, answering directly to EU citizens who are traditionally very careful with their personal data.

Furthermore, on 1 December 2009, the Lisbon Treaty took effect, nearly doubling the power of the European Parliament, and requiring the Council to submit legislation to be accepted, amended, or rejected by Parliament. One EU diplomat close to the talks told the press, "What all parties must realize is that since the Lisbon treaty came into force in December (2009), the European Parliament has real powers over international agreements and has to be negotiated with as an equal."[31] Indeed, that is why the Council rushed to push the interim agreement through on 30 November 2009, just one day before the Lisbon Treaty took effect. Although they were subsequently asked to contribute, many members of Parliament were angered and insulted by their initial exclusion from the project, and a majority voted against the plan. Their flat-out rejection of the plan, instead of postponing the vote until they learned more, begs the question as to whether Parliament's vote was intended to prove a point, or signaled a fundamental disapproval of the legislation.

Although several of the comments from members of Parliament after the vote seem to point to the first theory, celebrating the defeat of the "bully"[32] and declaring that it "will not tolerate being treated as a junior

DATA PROTECTION IN THE EU: KEY REGULATIONS

European countries are known for their strict approach toward data protection due to their experiences under World War II-era fascist governments and postwar Communist regimes. In comparison to U.S. data protection (*Datenschutz*), EU data protection is guided only by a few comprehensive regulations, including:

1. The Charter of Fundamental Rights of the European Union enshrines certain political, social, and economic rights for European Union citizens and residents into European Union law. It entered into force with the Lisbon Treaty. Chapter II, Freedoms, Article 8 focuses on the protection of personal data: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legiti-mate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

2. Directive 95/46 is the backbone of European privacy law. It is to ensure the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. According to Article 25 of the Directive, any cross-border transfer of personal information is only allowed if it has been decided that the third country provides an "adequate level of protection" in terms of the standards applied in the EU. The directive sets up a stringent process, whereby information trading practices with third countries, such as the United States, are evaluated by two committees, undergo a 30 day period of scrutiny by the Commission if necessary, and then are deemed compliant or non-compliant with EU laws.

3. Regulation 45/2001 deals with the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. For example, such data have to be processed fairly and lawfully; collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed.

4. Directive 2002/58 (E-Privacy Directive) concerns the processing of personal data and the protection of privacy in the electronic communications sector. It regulates a number of important issues such as confidentiality of information, treatment of traffic data, spam, and cookies.

For further information see: EU Commission, Freedom, Security, and Justice, <http://ec.europa.eu/justice_home/fsj/privacy/>.

partner,"[33] the tone in many of the comments regarding the SWIFT program indicated a belief that it was not only non-compliant with European regulations for data security, but that it was not clear that the data transfers were even necessary. Jens Geier, speaking for the Committee on Civil Liberties, Justice, and Home Affairs, said, "The effectiveness of the agreement is not entirely substantiated."[34] According to him, federal investigators in Germany have claimed that the information provided by the U.S. to the EU, as a result of the SWIFT program, was not effective in fighting terrorism. Although the vote was not public, statements made by German members of Parliament and Council, especially representatives of the Socialist, Green, and FDP parties, expressed their disagreement with the fundamental effectiveness of the agreement. The SWIFT program found a form of support, however, from the CDU in Germany. The German Minister of the Interior, Thomas de Maizière (CDU), abstained from the Council vote in November 2009, effectively allowing the SWIFT program extension to proceed. The CDU's coalition partner, the FDP, expressed outrage at the decision, saying that any vote but a "No" vote from Germany was a violation of their coalition agreement.[35] But German politicians were not alone in denouncing the program. Other states also voiced their equivocation. Supporters of the interim agreement argued that the "no" vote signaled that Parliament was missing the point. The risk of no deal between the U.S. and the EU was worse than the temporary deal, which had been negotiated by the Council. Council president-in-office Alfredo Pérez Rubalcaba argued that the TFTP was "a tool of great value which has made it possible to prevent terrorist attacks." He believed the accord provided sufficient guarantees on data protection.[36] Even beyond the basic assertion that the program was crucial to Europe's security, Cecilia Malmström, Member of the European Commission responsible for Home Affairs, warned Parliament that the temporary agreement with the U.S. had built in safeguards, which will be harder to include in the bilateral agreements the U.S. will negotiate, and that the accusations regarding the legality of the program, like that it gives away "virtually all data," are incorrect.[37] Malmström referred to the second Bruguière report to reinforce the necessity of the program saying, "The Report confirms that TFTP has been used to identify and arrest individuals who have subsequently been convicted of terrorist offences in our Member States," citing the Mumbai attacks of November 2008 and the 2006 Heathrow Airport transatlantic liquid bomb plot as successful interventions. The European Conservatives and Reformists Group in Parliament underlined her view on the uncertainties of unilateral U.S.-

LEGISLATIVE BODIES OF THE EUROPEAN UNION

The European Parliament is made up of 736 Members elected in the 27 member states of the enlarged European Union. Members of Parliament (MEP) have been elected by direct universal suffrage for a five-year period. They represent the interests of EU citizens. As of 1 December 2009, the Parliament's powers have doubled under the Lisbon Treaty, making it equal with the Council. When the Council rushed to pass the SWIFT extension before the Parliament gained its new powers, many interpreted it as a subver-sive measure, designed to keep Parliament from exercising its due right to provide a balance to the Council.

The Council of the European Union is the other arm of the Union's bicameral legislature. Its members represent member states with a rotating Council presidency, held by each member state in turn for a six month period. Each president presents his/her program to the Parliament and initiates debate with the members. He/she also gives a final report at the end of the term. Since members are representing the governments within the EU, and are not directly elected by the citizens, their priorities can vary widely from those of the electorate. The SWIFT case demonstrates how divergent the goals of these two different constituencies can be.

The European Commission is the executive branch of the Union. It is independent of national states and represents the union. It presents, explains and defends its legislative proposals to the parliamentary committees, and must take account of the changes called for by Parliament. It is answerable to Parliament and can be vetoed by it as well.

EU country agreements as well as the relative strength of the Council's agreement. "MEPs have cut off their noses to spite their faces. The USA will still be able to access most of this information, without many of the safeguards built into this agreement. Instead of negotiating an agreement at EU level, the USA will undoubtedly find it easier to negotiate with national governments."[38]

Thus, supporters of the interim agreement warned that, not only is the program providing real results, but even if opponents to the agreement did not subscribe to the results of the Bruguière report and the effectiveness of the SWIFT program, their rejection of the plan showed division and weakness in Brussels. The *Frankfurter Allgemeine Zeitung (FAZ)* put it like this: "Now the Obama administration may have to regard 'Europe' as a bunch of wobbly regional politicians who can't be trusted when it comes to drying up the streams of international terror finance."[39] Indeed, Parliament's resolution on SWIFT spent the majority of its time spelling out its legal concerns regarding the existing program and seemed to downplay the fears regarding the negative side effects of rejecting the proposal by almost encouraging bilateral agreements with the U.S.

The Way Ahead

SWIFT has said that it "has always, and will continue, to comply with the laws of the countries in which it operates […] The European Parliament's rejection of the interim agreement will have no impact on this situation."[40] In case a broad agreement with the EU on SWIFT data cannot be concluded, the U.S. could thus negotiate a deal with a country holding a server, either the Netherlands or Switzerland. Alternatively, the U.S. could use existing channels such as bilateral agreements on mutual legal assistance with each of the EU's 27 nations, which allow for the exchange of data within the laws of each national government. On first sight, this seems to be not a bad option for the U.S., which has shown a willingness to encourage cooperation by holding out other valuable incentives, like the Visa Waiver Program,[41] where countries participating in the program must comply with U.S. requests for personal data for all recipients of visas. However, bilateral deals are complicated, time consuming to negotiate, and leave a lot of holes, not guaranteeing the same full access to information.

Quickly concluding a new data sharing agreement would also be in the interest of the EU. Bilateral contracts would not only be difficult for the EU to monitor, but they would also mean taking a step away from the previous efforts of the Union to have a unified voice on the matter of data protection. In addition, the EU Parliament could signal its commitment to the international fight against terrorism and demonstrate that it is not "a bunch of wobbly politicians" as described by the *FAZ*. Doing so would strengthen their credibility in the area of international security and prove to the U.S. and others that Europe is not a divided voice. Moreover, a quick resolution and new agreement would absolve them from political finger-pointing, should another terrorist attack occur when there is no agreement in place.

Discussions about a new agreement on both sides of the Atlantic have therefore already started. In a meeting with members of the European Parliament in mid-March, members of the U.S. administration, including Deputy Secretary of State James Steinberg, assured that they were not planning to conclude bilateral agreements but wanted an agreement with the EU as a whole.[42] Malmström conceded in late March that "terrorism remains among the main threats that EU security has to face and we need to put in place tools that are up to the task, allowing for effective international cooperation. […] The program we propose to sustain with this EU-U.S. agreement on the transfer of financial messaging data proved its effectiveness in the past, and I am confident that it will continue to do so."[43] Together with her colleague Justice Commissioner Viviane Reding, she promised the highest possible level of protection for EU citizens' personal data through regular review processes and making sure that requests for data must be approved by a judicial public authority. Furthermore, Reding underlined: "We need to have our European citizens having a right of redress in the U.S., like American citizens have here in Europe, and the collection of this private data has to be proportional and to the point."[44] In addition, the two Commissioners envisioned a reciprocal element within the new agreement, asking the U.S. to share bank transfer data belonging to U.S. citizens in order to assist European antiterrorism efforts. However, for Malmström and Reding to begin serious talks on the collapsed deal, the EU's member states need to give them a negotiation mandate.

According to the draft negotiation mandate, transfer requests from the U.S. Treasury will have to be approved by a designated judicial authority in the EU. The specifics, however, are yet to be defined. Addressing the criticism of the European Parliament, the mandate also aims at prohibiting data-mining, i.e., the wholesale search of vast databases for patterns. In addition, the data may only be used for terrorism investigations. The mandate also foresees the possibility of establishing a European scheme modeled on the U.S. Terrorist Finance Tracking Program (TFTP). The idea behind an EU TFTP is that the EU could conduct its own investigations and analyses, which it then could share with the U.S., making both countries more equal partners. In mid-April, Reding and Malmström discussed the forthcoming negotiations with Janet Napolitano, the U.S. Secretary of Homeland Security, and Eric Holder, the U.S. Attorney General.[45] Malmström lauded the mandate for its ambitious yet pragmatic approach "which covers additional measures for shoring up data protection, ensuring that the fight against terrorism is the sole purpose, and also equipping ourselves with due compensation mechanisms."[46]

On 23 April 2010, when the EU Justice and Home Affairs Council was scheduled to vote on a mandate for the European Commission to negotiate bank data sharing through the SWIFT network by the end of June, not all EU parliamentarians were satisfied. The MEPs welcomed that the new EU Commission negotiation mandate explicitly recognized a role for Parliament in the decision on SWIFT data transfers. Nonetheless, the issues at large were still bulk data transfers and the possibility of judicial remedy for Europeans in the United States, i.e., whether EU citizens would have a right of appeal to the American authorities if their personal data were misused. "The problem of mass data transfers and long data storage has not been

solved yet within the new mandate," criticized German Socialist Parliamentarian Birgit Sippel, continuing: "Furthermore, strict conditions for transferring the data to third countries were missing."[47] And rapporteur Hennis-Plasschaert complained that "with these guidelines we are still talking about massive data transfers...Even with this new mandate the idea would be to transfer 90 million pieces of data each month."[48] While both argued for more targeted data transfers, the Commission believes that the principle of bulk transfers would have to be maintained for technical reasons and to ensure effectiveness.

The vote was eventually postponed because of the volcanic eruption in Iceland and travel restrictions all over Europe; formal approval is expected to take place in the Council on 10 May. Only once EU ministers approve the mandate can talks with the U.S. begin. Once an agreement is reached, member states and the Parliament will have to approve it; the vote on the new agreement is tentatively set for July. It remains to be seen whether the Parliament will be more cooperative this time.

NOTES

For a timeline of events concerning SWIFT, see <EU Parliament, The SWIFT Dossier in Parliament since 2006, see <http://www.europarl.europa.eu/news/expert/background_page/019-68530-032-02-06-902-20100205BKG68527-01-02-2010-2010-false/default_p001c003_en.htm>.

1 Quoted in: "Justizministerin sieht keine Sicherheitslücke durch Swift-Scheitern," 12 February 2010, <http://www.toptarif.de/news/finanzen/12022010-justizministerin-sieht-keine-sicherheitsluecke-durch-swift-scheitern>.

2 Quoted in: "MEPs Say 'no' to SWIFT, EurActiv," 11 February 2010, <http://www.euractiv.com/en/justice/meps-say-no-swift>.

3 Quoted in: "U.S. Urges European Parliament to Back Data Deal," *Der Spiegel*, 8 February 2010, <http://www.spiegel.de/international/world/0,1518,676524,00.html>.

4 Ibid.

5 Patryk Pawlak, "Made in the USA? The Influence of the U.S. on the EU's Data Protection Regime," *CEPS Liberty and Security in Europe*, November 2009.

6 Adam Szubin, the U.S. Treasury Department official in charge of the Terrorist Finance Tracking Program quoted in: "U.S. Urges European Parliament to Back Data Deal," *Der Spiegel*, 8 February 2010, <http://www.spiegel.de/international/world/0,1518,676524,00.html>.

7 "Terrorist Finance Tracking Program Fact Sheet," U.S. Department of the Treasury, Press Room, 23 June 2006.

8 Eric Lichtblau and James Risen, "Bank Data Sifted in Secret by U.S. to Block Terror," *The New York Times*, A-1, 23 June 2006; Barton Gellman, et al., "Bank Records Secretly Tapped," *The Washington Post*, A-1, 23 June 2006; Josh Meyer and Greg Miller, "U.S. Secretly Tracks Global Bank Data," *Los Angeles Times*, A-1, 23 June 2006; and Glenn R. Simpson, "Treasury Tracks Financial Data in Secret Program," *Wall Street Journal,* A-1, 23 June 2006. As reported by CRS Report to Congress, 7 July 2006.

9 European Parliament, "Parliament's Rejection of the SWIFT Agreement," 3 March 2010, <http://www.europarl.europa.eu/news/expert/background_page/019-68530-032-02-06-902-20100205BKG68527-01-02-2010-2010-false/default_en.htm>.

10 A subpoena is defined as an order directed to an individual commanding him to appear in court on a certain day to testify or produce documents in a pending lawsuit. The U.S. government has the right to subpoena information from its nationals or from foreign nationals operating on its soil. Foreign corporations can be interpreted to be "persons" in this context, thus subject to the subpoenas.

11 "Terrorist Finance Tracking Program Fact Sheet," U.S. Department of the Treasury, Press Room, 23 June 2006.

12 Chapter 35 – International Emergency Economic Powers, U.S. Code Title 50, Chapter 35, <http://www.law.cornell.edu/uscode/50/usc_sup_01_50_10_35.html> (23 March 2010).

13 Ibid.

14 Jennifer Elsea and M. Maureen Murphy, *Treasury's Terrorist Finance Program's Access to Information Held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, Congressional Research Service Report to Congress, 7 July 2006.

15 Michael P. Malloy, *United States Economic Sanctions: Theory and Practice* (The Hague, Netherlands: Kluwer Law International, 2001), <http://www.enotes.com/major-acts-congress/united-nations-participation-act>.

16 Executive Order 13224 of 23 September 2001, <http://www.fas.org/irp/offdocs/eo/eo-13224.htm>.

17 Chapter 35 – International Emergency Economic Powers, U.S. Code Title 50, Chapter 35, <http://www.law.cornell.edu/uscode/50/usc_sup_01_50_10_35.html> (23 March 2010).

18 Quoted in: CRS Report to Congress, 7 July 2006.

19 "Processing of EU Originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — SWIFT." 20 July 2007, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:166:0018:01:EN:HTML>.

20 "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," *Journal of the European Union*, 23 November 1995, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

21 The United States Mission to the European Union Press Release, "U.S., EU Reach Agreement on SWIFT Terrorist Finance Data," 29 June 2007, <http://useu.usmission.gov/Dossiers/Terrorist_Financing/Jun2907_SWIFT_Deal.asp>.

22 Remarks by Cecilia Malmström on the debate over SWIFT, 10 February 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/24&type=HTML>

23 SWIFT Statement, SWIFT Respects Data Protection Legislation, <http://www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2008/swift_respects_data_protection_legislation.page?> (12 March 2010).

24 The United States Mission to the European Union Press Release, "U.S., EU Reach Agreement on SWIFT Terrorist Finance Data," 29 June 2007.

25 SWIFT Statement on the European Parliament's Rejection of the Interim EU-U.S. Agreement on the Terrorist Finance Tracking Programme, 11 February 2010, <http://www.swift.com/about_swift/press_room/swift_news_archive/2010/data_privacy/SWIFT_statement_EU_Parliament_Rejection.page> (12 March 2010).

26 SWIFT Statement on its Distributed Architecture Solution, <http://www.swift.com/solutions/industry_initiatives/distributed_architecture.page> (12 March 2010).

27 "The European Parliament Shoots down the EU/U.S. SWIFT Agreement to Protect Civil Liberties," *The New Federalist.EU*, 12 March 2010, <http://www.thenewfederalist.eu/The-European-Parliament-shoots-down-the-UE-U.S.-SWIFT-agreement-to>.

28 European Parliament, Parliament's Rejection of the SWIFT Agreement, <http://www.europarl.europa.eu/news/expert/background_page/019-68530-032-02-06-902-20100205BKG68527-01-02-2010-2010-false/default_p001c001_en.htm> (18 March 2010).

29 "EU, U.S. Re-assess SWIFT Data-sharing Deal," *EurActiv*, 18 March 2010, <http://www.euractiv.com/en/financial-services/meps-washington-collapsed-data-sharing-deal-news-355141>.

30 European Parliament, "Parliament's Rejection of the SWIFT Agreement," 3 March 2010, http://www.europarl.europa.eu/news/expert/background_page/019-68530-032-02-06-902-20100205BKG68527-01-02-2010-2010-false/default_en.htm>.

31 "2nd Update - EU Lawmakers Reject EU-U.S. Data Sharing Plan," *Dow Jones Business News*, 11 February 2010.

32 GUE/NGL President Lothar Bisky Speaking Following the SWIFT Vote in the European Parliament, <http://www.guengl.eu/showPage.jsp?ID=8212&PRINT=1&M=-1&Y=-1>.

33 UK Green MEP and EP Civil Liberties Committee Member Jean Lambert.

34 Jens Geier, Mitglied des Europäischen Parlaments Press Release, 4 February 2010, <http://www.jensgeier.eu/meldungen/18002/80288/Europaeisches-Parlament-zeigt-Zaehne—-EU-Parlament-lehnt-SWIFT-Abkommen-ab.html>.

35 Thorsten Jungholt, "Swift-Abkommen: FDP warnt Union vor Koalitionsbruch," *Welt Online*, 29 November 2009, <http://www.welt.de/die-welt/politik/article5320498/Swift-Abkommen-FDP-warnt-Union-vor-Koalitionsbruch.html>.

36 European Parliament, "SWIFT: European Parliament Votes Down Agreement with the U.S.," 11 February 2010, <http://www.europarl.europa.eu/news/expert/infopress_page/019-68675-039-02-07-902-20100209IPR68674-08-02-2010-2010-false/default_en.htm>.

37 Remarks by Cecilia Malmström, European Parliament, Debate on SWIFT, 19 February 19, 2010.

38 Timothy Kirkhope MEP, European Conservatives and Reformists Group Coordinator on Justice and Home Affairs, quoted in: "Swift Agreement's Rejection: MEPs Have Cut off their Noses to Spite their Faces," 11 February 2010, <http://www.ecrgroup.eu/swift-agreement—039-s-rejection—meps-have-cut-off-their-noses-to-spite-their-faces-news-63.html>.

39 "Good News at Last from Europe," *Der Spiegel*, 12 February 2010.

40 SWIFT Statement on the European Parliament's Rejection of the Interim EU-U.S. Agreement on the Terrorist Finance Tracking Programme, 11 February 12010, <http://www.swift.com/about_swift/press_room/swift_news_archive/2010/data_privacy/SWIFT_statement_EU_Parliament_Rejection.page>.

41 European Parliament, "Resolution on SWIFT, the PNR Agreement and the Transatlantic Dialogue on These Issues," 11 February 2010. After 9/11, the U.S. changed its rules for the Visa Waiver Program. It now requires pre-approval for travel, including the transfer of personal data, which has caused concern among countries recently applying for membership, like Hungary and Greece.

42 "2nd Update - EU Lawmakers Reject EU-U.S. Data Sharing Plan," *Dow Jones Business News*, 11 February 2010.

43 Quoted in: Paul Meller, "EC Proposed Compromise over SWIFT Bank Information Sharing," C*omputer World UK*, 25 March 2010, <http://www.computerworlduk.com/management/government-law/public-sector/news/index.cfm?newsid=19582> (26 March 2010).

44 Quoted in: "Brussels to Push for Stronger Privacy Safeguards in EU-U.S. SWIFT Deal," *M&G News*, 23 March 2010.

45 EurActiv, "EU to Launch Anti-terror Finance Tracking Plan," 25 March 2010, <http://www.euractiv.com/en/financial-services/eu-launch-anti-terror-finance-tracking-plan-news-376447>; Constant Brand, "MEPs Seek to Limit Bank Data Shared with U.S.," *European Voice*, 4 April 2010, <http://www.europeanvoice.com/article/2010/04/meps-seek-to-limit-bank-data-shared-with-us/67615.aspx>

46 Quoted in: "EU Seals Mandate for Negotiating new Agreement with U.S. on Transfer of Bank Data," *Presidencia Espaniola*, 23 April 2010, <http://www.eu2010.es/en/documentosynoticias/noticias/abr23_consejointerior.html>.

47 Quoted in: "Neuverhandlungen über SWIFT: EU-Abgeordnete warnen vor ungeprüftem Massentransfer von Bankdaten," Europäisches Parlament, Informationsbüro Österreich, <http://www.europarl.at/view/de/AKTUELLES/press-release/pr-2010/pr-2010-April/pr-2010-Apr-3.html;jsessionid=A01133D55B609E1CB28F163B38237CFB> (23 April 2010).

48 Quoted in: "SWIFT is Back: MEPs Want to Limit Transfer of Financial Data," European Parliament, 4 April 2010, <http://www.europarl.europa.eu/news/public/story_page/019-72113-096-04-15-902-20100406STO72100-2010-06-04-2010/default_en.htm>.

The fight against terrorism has been on the forefront of the U.S. and German agendas and shapes the relationship between both countries. While differences in counterterrorism policy exist, the U.S. and Germany have also very successfully cooperated in counterterrorism measures. This publication examines some of those differences, namely the disagreement between the U.S. and EU over sharing private financial data. It looks at the legal situation in the United States and the political struggles in the European Union that hamper better cooperation across the Atlantic, and offers ideas on how the two actors can overcome their differences on data-sharing and SWIFT. This Issue Brief is part of AICGS' larger project on "Political, Cultural, and Economic Origins and Consequences of International Terrorism: American and European Answers."

AICGS is grateful to the Fritz Thyssen Stiftung for its generous support of this Issue Brief and project.

Recent Publications from AICGS:

- Frank Gadinger and Dorle Hellmuth, Finding Security in an Age of Uncertainty: German and American Counterterrorism Policies, AICGS Policy Report 41 (2009).

- Kirsten Verclas, *Transatlantic Counterterrorism Policy: Cultural, Economic, and Financial Aspects*, AICGS Issue Brief 34 (December 2009).

Edna Dretzka is currently a Robert Bosch Fellow at the Stiftung Wissenschaft und Politik in Berlin
Dr. Stormy-Annika Mildner is a Senior Research Fellow in the Research Unit the Americas of the Stiftung Wissenchaft und Politik.

Anything but SWIFT: Why Data Sharing is Still a Problem for the EU

AICGS
AMERICAN INSTITUTE FOR CONTEMPORARY GERMAN STUDIES
AT JOHNS HOPKINS UNIVERSITY

1755 Massachusetts Ave., NW
Suite 700
Washington, D.C. 20036 – USA
T: (+1-202) 332-9312
F: (+1-202) 265-9531
E: info@aicgs.org
www.aicgs.org