ROCZNIKI KULTUROZNAWCZE
Tom IV, numer 2 – 2013

MICHELLE FRASHER

VIOLENCE, LAW AND CULTURE: THE SOCIAL CONSTRUCTION OF US AND EUROPEAN PRIVACY IDENTITIES AND TRANSATLANTIC COUNTER-TERRORISM COOPERATION

Social constructivist theory, or constructivism, emphasizes the role of ideas in shaping institutions (governments, agencies, international organizations) and processes (policies, procedures, norms of behavior) believing that they are the results of actions and interactions among societies shaped by historical experience and culture (Wendt, 1992; Ruggie, 1998; Hopf, 1992). In the post 9/11 atmosphere, differences among US and European attitudes regarding political violence have been at the forefront of scholarship and public commentary, but few have addressed how cultural perspectives of privacy have affected transatlantic data sharing in counter-terrorism cooperation. Constructivism demonstrates how historical experience has shaped US and EU privacy identities – their beliefs and ideas about the protection of an individuals' data, which affects how states share information to combat political violence. Ideas about privacy and data sharing to combat political violence often represent a "trade off between security and liberty" (Katzenstein, 2002) where societies may choose between protecting themselves from treats and safeguarding private information. As sharing data across borders has become an important component of counter-terrorism (CT) operations, the differences among transatlantic privacy identities will affect cooperation in the "War on Terror."

Privacy identities have been shaped by historical episodes of violence. European experiences with state-led surveillance and domestic terrorism

MICHELLE FRASHER, Ph.D.—Assistant Professor, Department of History and Political Science, Molloy College; address for correspondence—e-mail: mfrasher@frasher.cc

during the Second World War and Cold War eras have created a cultural consciousness that frames the EU's privacy identity as a fundamental human right. These episodes have also influenced how Europeans perceive terrorist threats. Because Europe typically dealt with political violence from home, CT strategies emphasized criminal procedures entrenched within the legal system, which required officials to take notice of national privacy and data protection protections in their investigations.

The US did not encounter political violence during World War II on the home front and had little contact with domestic terrorism during the Cold War. The US government combated terrorism abroad with military intervention, covert action, and sanctions against states who supported these groups. America's Cold War role as the defender of democracy against global encroachments by Soviet Communism was heavily intermeshed with its privacy identity too. Despite assertions that the US privacy identity is protective of intrusions by the government, it has been heavily permissive of covert data collection and surveillance on its citizenry and foreign nationals for national security purposes. Generally, American law sees privacy as property based, and protects data in the possession of the holder, no matter what entity this might be, so legislation has only selectively regulated data usages.

The variances in privacy identities are important to contemporary CT operations because as information technologies have spread with globalization, national privacy identities, legal systems, and security concerns increasingly overlap and clash. Access to data can assist governments and law enforcement to map political violence within states and across sovereign boundaries so data sharing is a key feature of security policies. Yet, US and EU officials want to promote cooperation in CT, and the need for security may provide for a new transatlantic standard of data sharing that accommodates both privacy identities.

Thus, the historically and socially constructed identities that have produced laws that govern data sharing in the EU and US will impact their domestic and foreign relationships. Yet, constructivism tells us that institutions and procedures are the result of interactions *within* societies and *among* societies so it is reasonable to assume that *both* US and EU privacy and security values will have a hand in molding the future of transatlantic CT cooperation.

SOCIAL CONSTRUCTIVISM: FORMING IDENTITIES

Among the main schools of thought for international relations, all of which consider the sources of interstate behavior—why governments act they way they do—constructivism is primarily concerned with the way societies develop ideas, ideologies, and identities and how these factors impact the formation of institutions (international organizations, governments) and norms (standards of behavior and law). It maintains that human action and consciousness have a role in the politics of international life (Ruggie, 1998).

These views are critical of the two dominant paradigms of international relations—neorealism and neoliberalism. Both theories believe that the world operates in a condition of anarchy—an international system without a government above the power of states to make and enforce laws. Neorealism believes anarchy creates a Hobbesian-esque conflict-ridden world where all states must protect themselves from the interests of others by building military strength and making (temporary) alliances to maintain their security. All states behave for the same reasons, to protect their sovereignty, regardless of the type of government or actions of individual decision-makers (Waltz, 1959, 1979).

Conversely, neoliberals see opportunities for states to get what they want through cooperation, whether it be with trade, investment, alliances, or through membership in international organizations. Some states will choose to share resources and create institutional bonds because it produces a mutual benefit. The presences of cooperation in the international system mitigates the effects of anarchy and emphasizes cooperation and diversity of choice among different types of government and among decision-makers (Baldwin, 1993; Keohane, 1986).

Neoliberal and neorealist perspectives explain interstate behaviors, yet they do not explain why states have these identities or interests—they are simply assumed as given. Surely we cannot relegate all societies and the behaviors of states to the predestined interests ‘inherent’ in the system. As Alexander Wendt put it, “*Anarchy is what states make of it*” (1992, p. 395). Governments and their societies have identities that are formed by social interactions occurring within their borders that drive the creation of institutions and laws and are further molded in the context of their interactions with the international community. Each society has unique experiences that create identities imbued within their customs and governments, and they will see the world in these contexts.

This is where historical experience and culture play their greatest roles to explain the politics of transatlantic CT policies and the formation of privacy identities. Identity is an essential part of culture and it determines actions and methods. Neorealist and neoliberal traditions offer many perspectives as to why Europe and the United States want to protect themselves from the consequences of political violence, and why cooperation is mutually beneficial to counter these threats – loss of life, promotion of governmental stability, halting disruptions to the economy, a belief in the right of law and representative democracy as a means of political grievance, higher probability of stopping these attacks by sharing information, etc. However, Americans and Europeans have different views of the problem and ways of responding to it. How they see privacy in particular speaks to the heart of these differences. If political violence is shared transatlantic concern, why do they view the problem of information sharing in CT operations differently?

Constructivism explains the presence of differing privacy identities formed by unique experiences with terrorism. Although notions of privacy were constructed from many sources, key events in the 20th century involving acts political violence from the state and from national groups have played a large part to construct contemporary privacy identities which have affected CT cooperation. The fascist and communist threats of World War II and the Cold War molded US and EU identities in many respects and were defining moments for privacy and security too. Most importantly, both of these eras involved and contributed to the development of communications technologies, which have deeply impacted how the EU and US view and respond to threats. Advancements in communications and data transmission, gathering and analysis—satellites, radio, television, signals, high resolution cameras, computing—were developed and used during the Second World War and the Cold War to protect the state from threats and they altered how data is collected, used, and processed.

Advances in communications technology influenced cultural perceptions of privacy as it has helped to codify and automate data and made it easier to collect and analyze. The spread of international communications, especially in the last 50 years, has enabled personal data to leave sovereign boundaries which made it difficult to control and determine ownership. Technology then has affected how data has been *regulated*. Culture again plays a role. Hart and Kim (2001) noted that "each new technology 'encodes' a set of institutional and cultural practices in itself as part of the process of being accepted in dif-

ferent societies" (p. 5). Susan Strange (1990) declared that the mere presence of new means of communication was not enough, a society had to be willing to adopt them, and they most likely had a hand in shaping them at the same time. Technology in its creation, usage and regulation is subject to what cultures make of them (e.g. Cannataci, 2009). Thus, the development of communications technologies and how they have been used in the Second World War and the Cold War have shaped perceptions of privacy and its regulation.

War, political violence, and the evolution of communications technologies altered the social, political and strategic landscapes of transatlantic relations, and though there were certainly some common experiences, and the US and Europe share values and goals, it is the *differences* among these ideals that constructivism explains. These differences have produced varied privacy and security identities that describe why the US has favored national security over privacy, while the EU has bound the criminal investigation of political violence to the law and the individual's human right to privacy.

IDENTITIES: PRIVACY, DATA OWNERSHIP AND SECURITY

What events have driven the creation of privacy identities? First, we must define privacy. According to the *Oxford English Dictionary* it is "a state in which one is not observed or disturbed by other people" or "the state of being free from public attention." In this simplistic view, privacy involves elements of anonymity or freedom, but the term is extremely difficult to define because it is subject to cultural context. To paraphrase Wendt; *privacy is also what societies make of it*.

Yet, defining privacy is essential because it determines how governments will regulate access to data. Each society has ideas about what constitutes personal privacy. Once those definitions are established, they will determine the *ownership* of data. Ownership then becomes a framework for understanding the relationship between privacy and data protection. If conceptions of privacy determine data ownership, these ideals guide the legal dissemination of data, which lead to data protection laws to determine how, when, and if data can be collected, stored and accessed in accordance with society's perceptions of privacy. (Bignami, 2007).

As the following examination of the roles that history, political violence, and technology have played in the formation of these definitions suggest, US

experiences have produced a property view of privacy and therefore ownership of data is vested in the holder, whereas European law has been framed around human rights which places ownership in the hands of the individual.

Conceptualizations of terrorism have also involved social interaction. If security is the ability of the state to "be free from threat and the ability of states to maintain their identities" (Buzan, 2001, 432.) then each society will strive to achieve its security to preserve its ideas (Firat, 2010). In turn, how social groups define themselves will determine a state's "world view" and affect their perceptions about their place in the international community, what constitutes a threat to their identities and beliefs, and what strategies they will employ to protect them.

Shapiro and Byman (2006) believe that the US and EU perceive contemporary terrorist threats from organizations like Al Qaeda differently because of "near enemy" and "far enemy" distinctions. These classifications fit modern perceptions, and they reflect the historical construction of US and European responses to political violence as well. Europe has dealt with state sanctioned terrorism from the Nazi and Communist eras, and during the 1960s and 1970s was the target of many near enemy groups including left-wing and nationalist extremists. The threat of political violence typically originated from communities inside European borders, but these groups often had international ties. Dealing with a near and far enemy that perpetrated attacks on one's homeland made military action inappropriate. Terrorism became criminalized and placed within the purview of the police and court system. To do so required surveillance of the population which necessitated attention to privacy laws to pursue suspects.

American perceptions of the threat of terrorism were molded during the Cold War, where far enemy states supported far enemy groups to advance a foreign policy agenda. Terrorism became part of the Cold War rivalry and extremists from other countries targeted US citizens and interests abroad, so Americans responded with sanctions or military force. As a result, the military has been utilized mainly as the implimentor of counter-terrorist policy, the muscle behind the message. This has enabled the US to "pursue its counter-terrorism objectives in relative isolation from other domestic issues" (p. 38). In terms of privacy, surveillance was necessary to root out Communist subversives at home where agencies like the FBI and especially the National Security Agency (NSA) routinely kept tabs on citizens and those abroad to spy on the activities of the Soviet empire (Shapiro and

Byman, 2006). The US has frequently placed national security interests in front of the individual's rights to privacy.

Privacy and perceptions of the treat of terrorism are intertwined, and the struggle between them seems to represent the "trade off between security and liberty" (Katzenstein, 2002). But it would be false to characterize US concerns about privacy as nonexistent or that privacy legislation in Europe somehow makes the EU soft on terrorism (Hoffman, 1999). Both sides share genuine concerns about the threat the political violence poses to their values and security. When one views the history of European counter-terrorism operations and the EU's approach to security and privacy within the 1st and 3rd pillars we begin to see how the future of transatlantic data sharing will accommodate both views of privacy to create a new paradigm.

The 1992 Maastricht Treaty organized European integration into three "pillars," with each representing issue areas that assigned certain responsibilities to European institutions and national governments.

- Pillar I: economic, social, cultural, immigration and borders.
- Pillar II: common foreign policy and security
- Pillar III: police and judicial cooperation in criminal matters

The division of interests within the pillar structure presents challenges to CT cooperation which encompass several pillars, such as data sharing, but these discrepancies also create opportunities for cooperation. The majority of privacy and data protection legislation was created under the 1st pillar to protect individuals from governmental and private intrusions, and did not cover data protection in issues involving national security and criminal proceedings. These were negotiated elsewhere, and national sensitivities to 2nd and 3rd pillar issues have tended to be more guarded and resistant to the control of EU institutions. However, even as the private market (banks and airlines for example) must abide by 1st pillar privacy protections, their data is also of interest in 2nd and 3rd pillar police and security operations to follow financial transactions to track terrorist funding or finding persons of interest in airline passenger data.

The 2009 Lisbon Treaty abolished the pillar system to create a more integrated Union, but the legislation is still in the process of being amended. This creates opportunities for adaptations. Constructivism asserts that transatlantic social interaction will create a new paradigm that can accommodate American and European values and ideas. As the Europeans streng-

then their privacy identities regionally, they will also want to strengthen their ability to fight political violence which will require cooperation among the members of the Union, but also with the US. The US in turn, needs the EU's assistance to acquire data for its counter-terrorism operations and so it will have to adapt to Europe's culture of privacy.

HISTORICAL ORIGINS OF PRIVACY AND OWNERSHIP

Whitman (2004) noted that privacy law in Europe originated with the desire to protect the dignity of the nobility from media intrusions. Later, when European governments transitioned to democracies after the Second World War, these laws were extended to include privacy as a fundamental human right. In contrast, conceptions of privacy in the US developed through case law as a protection against invasions from the state on one's person and property to preserve liberty—freedoms of expression, the prohibition of quartering soldiers, the right to bear arms, etc. American law only regulated privacy in a sectoral manner, targeting certain issues or groups, and treated private data as a property of the holder.

Whitman presents constructivist foundations for US and EU privacy identities and their relationship to the law and the institutions that govern. "We have intuitions that are shaped by the prevailing legal and social values of the societies in which we live" (p. 1160). The structures of government reflect society's beliefs and serve as messengers through time. Constructivists would agree that identities are encoded into law and the interpretations of these laws (as well as the laws themselves) evolve with changes in social attitudes.

France and Germany provided the foundations of modern continental privacy laws, as governments established the practice of protecting the images of its nobility for personal honor. During and after the French Revolution, philosophers and officials debated the virtues of free speech with the value of maintaining honor and dignity. The Germans however were more comfortable with codifying these principles because they had developed a sense of self that was tied to data control, which made their conceptualizations of privacy easier to legislate. The right to personality, or *Personlichkeit*, was deeply rooted in German intellectual and theological history, where ideas about individual liberty and freedom were closely related to self-realization, or the right to control and create one's image in society

(Whitman, 2004; Sorkin, 1983). Nineteenth century German jurists and philosophers took inspiration from the Roman law of insult that included both material (property) and immaterial (dignity) rights. The courts extended material rights to the control of one's name, image, correspondence much like copyright. Responding to technological innovations like the telegraph, the right to control data was imbedded in informational copyright which married the tangible representations of ideas (writings, pictures) to self-creation. These ideas were introduced to the Civil Code in 1900 on a limited basis, and later selectively applied to citizens of the Nazi Reich to distinguish the rights of racially "pure" Germans from others (Whitman, 2004). Thus, ideas of identity, data control, and privacy were very much tied to social interaction and the rights of ownership to the individual.

The American Constitution does not mention privacy explicitly, but the Supreme Court has recognized that the right to privacy exists implicitly in the Bill of Rights in several Amendments including the right of association and the right to be free from unreasonable searches and seizures. Generally, the legalities of US privacy and data protection have been built on common law (case law, or law set by precedent) in the form of torts, usually civil complaints brought forward seeking damages for an action (Wade, 2010). Privacy identity has rested upon protections from intrusions from the state rather then the private sector, which has been largely untouched.

But there are historical, and to some, legal, congruencies between US and European views. One of the earliest examples came from Samuel Warren and Louis Brandeis in 1890 in *"The Right to Privacy"* written in response to the media's reporting of a party given at the Warren's household. The two lawyers (Brandeis was later appointed to the Supreme Court) horrified at the press's intrusions, defined the right to privacy as "the right to be left alone." They referred to European ideas of honor and reputation, but could not cite a precedent for the violation of one's person through insult in the American traditions of law. However, they did see the protections of one's rights to "intellectual and artistic property" as sufficient to extend to the protection of "personal space." The article took inspiration from Germany, but stopped short of the right to personality.

Whitman and other legal scholars commonly cite this as the point of origin for America's property-based privacy identity. However, others have argued that the Warren and Brandies article did introduce personhood as a central tenant of American privacy right. Bloustein (1964) believed US tort laws on all aspects of privacy served to create a right to privacy based on

"human dignity." Simmel (1968), Reiman (1974) and Schoeman (1992) agreed, and supported a right to personality that included individuality, dignity, and freedom that placed privacy as part of a "complex social practice" where an individual communicates and society recognizes "that his existence is his own." Based on these interpretations of US law, it seems then that there is a basis for shared transatlantic ideals.

PRIVACY AND SECURITY: WORLD WAR II AND THE COLD WAR

So US and European privacy identities originate from differing social interactions, but there are some shared values. In the 20th century, violence makes a firmer imprint on the subject, again with distinct consequences. Unfortunately, Whitman did not put much faith into how these identities, and the laws that reflect them, had been altered by political violence or the spread of communications technologies in the last 60 years. Instead, he characterized the Nazi period as prompting a post-war "leveling up" of Europe's long-established privacy principles. This analysis downplays the role of the state and technology in shaping contemporary continental ideas though. We must, in the information age, take the ideological influences of violence and technology into account if we are to understand how these ideas have brought evolutionary changes to US and European privacy identities, and affected transatlantic cooperation against the current wave of political violence.

The clearest example of how privacy, data collection and technology converged to threaten the personal freedoms of individuals, and shape perceptions of terrorist threats, can be seen during the Third Reich (although we could easily include the oppression of the Soviet state in this analysis). Widely characterized as a form of state terrorism (Sedgwick, 2007), the Nazis enveloped all aspects of life and enforced their rule through systematic intimidation, violence, and fear. The state attempted to create a registry of its citizenry, to include all aspects of their lives from addresses, occupations, religion, genealogy, to eugenics. The Nazi party and all levels of government employed a myriad of methodologies to collect and analyze data from censuses, police registrations, questionnaires, draft cards and so on to create these personal profiles which were used in part to locate groups for deportation, encampment, labor, and extermination (Luebke and Milton, 1994). However, the bureaucratic organization of the Reich was dispersed

among many levels of party involvement and local, state and federal government and the catalogue was never realized. The decentralization of the Nazi state could not create a cohesive and *standardized* process for data collection for everyone within its borders, and it could not consistently identify specific individuals and groups within German territories. Technology's role in this process, through the use of punch card machines to analyze census data and locate targeted populations, is controversial though. In truth, there were many reasons that led to the destruction of populations—prejudices, fear of retribution from the state, and citizen compliance to name a few (Luebke & Milton, 1994; Allen, 2002; Seltzer, 1998). However, its use in the tabulation of data like processing the German census and recording members of the concentration camps, along with the other communications advancements developed during the war like sonar, radio (e.g. HRO receivers), and radar were early examples of the potential uses implied by the codification and computerization of data collection that would make it easier to collect, disseminate and analyze information in the information age.

Nor was the misuse of data limited to European governments during the War. The US saw little violence within its borders with the exception of the attack on Pearl Harbor and isolated skirmishes in the Alaskan territories. Yet, recent evidence from US archives has shown that the Justice Department and Secret Service received data from the 1940 census to locate Japanese-Americans for transference to detention camps. Considering citizens of Japanese heritage as possible near enemy interlopers for the far enemy invaders, these internments were mandated by Roosevelt's Executive Order 9066 which allowed the Department of War to designate certain areas of the US as military zones. The Census Bureau acted legally since the Second War Powers Act enabled data sharing for purposes of national security (Seltzer & Anderson, 2007).

These experiences with violence and the misuse of personal data by the state left a lasting imprint on the political, economic, social and cultural norms of European governments and the international institutions of the post-war era. In the 1948 United Nations Universal Declaration of Human Rights, Article 12 placed privacy issues firmly in the scope of human rights stating that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." This passage nods to both American and European privacy identities because it takes into account both property and dignity.

But it was Germany's idea of *Personlichkeit* that became ingrained in the EU's privacy ethos, in its regional institutions, and its national practices (Coors, 2010, O'Cinneide et. al., 2006). The 1950 European Convention on Human Rights (ECHR) defined the parameters of privacy in Article 1, "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 2 established the security allowances of privacy protection—"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (Council of Europe)."

As a result, Europe established comprehensive data protection guidelines and laws with an eye to the development of technologies that made it easier to spread information, and harder for individuals to maintain their control over it. Much of these efforts began in the 1960s when the governments and private companies, mostly telecommunications providers and banks, began to store large amounts of data. As the governments expanded the welfare state, protections for privacy were also extended to the health, education and benefit systems (Bennett and Raab, 2003). The Council of Europe helped states ameliorate differences among their legal structures, and in 1981 Convention 108[1] provided frameworks for standardizing the collection and processing of data via automated means, provisions for the legal storage, accuracy, confidentiality, and disclosure of an individual's data from both private and public sources. These rules were to be implemented within each of the contracting states but ratification and implementation was slow.

These efforts paved the way for the EU to enact more binding measures with Directive 95/46/EC in 1995 which "applies to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non automated filing systems (traditional paper files)" and established guidelines to determine the lawful processing of this data. These rights included the right to access one's own data and the right to object to the processing of data (Directive, 1995). To insure that governments or other entities could not target populations again, individuals owned the rights to their personal data which constituted their identities, and

[1] Formally known as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

they were in control of how they conveyed those identities to others. Thus, they should be able to consent to the collection and use of their personally identifiable information, which can include their name, face, date and place of birth, credit card numbers, and genetic information. 95/46/EC was enacted under the 1st pillar of integration so it did not include data collection for national security, criminal investigations, or the judiciary. However, it did distinguish itself from US laws because it vested data ownership to the individual no matter what entity possessed that data. Because it as a Directive rather than a law that enabled EU institutions authority to enforce it, it was the responsibility of each member state to enact national laws to support the Directive and set up domestic institutions to insure compliance.

The United States also considered the effects of technology on privacy and data management in the post World War era, but continued to pursue a sectoral and property based strategy, and made significant allowances for domestic surveillance for national security.

Most privacy laws regulated access to data and rarely limited government collections. Among the most notable regulations were the 1954 Census Confidentiality Statute that restricted the uses of census data that would enable an individual to be identified and used for any other purpose than originally intended; the 1966 Freedom of Information Act and the 1974 Privacy Act set standards of disclosure for government records; the 1980 Privacy Protection Act disallowed law enforcement to conduct searches and seizures on publishers unless these works were related to a crime "to which the materials relate"; the 1994 Driver's Privacy Protection Act restricted the disclosure of personal information in a state's department of motor vehicles; the 1997 Taxpayer Browsing Protection Act prohibited IRS employees from accessing confidential taxpayer information; and the 2002 Federal Information Security Act (FISMA) regulated and standardized types of data collection and storage within the federal government (CDT.org).

Generally, the US eschewed regulating data held by private companies because it feared this would curtail commerce and investment. As a result, privacy and data protection laws were usually concerned with ensuring data accuracy and procedures for disclosure for criminal and national security investigations.

Still, none of this legislation addressed the virtually unfettered collection of data during the Cold War that violated the Fourth Amendment which protects citizens from unreasonable searches and seizures, among other freedoms. The clandestine National Security Agency (NSA) used electronic

surveillance to gather information from private companies and monitored telephone and cable traffic within the US and from individuals having contact with foreign nationals with very little supervision. With the 1978 Foreign Intelligence Surveillance Act (FISA) Congress put some limits on the organization with a Foreign Intelligence Surveillance Court which reviewed and approved all requests for data and approve them (National Security Archive, 2006). Yet, the Court rarely denies these applications and the majority of these requests are kept secret (Movius and Krup, 2009).

The NSA was not the only agency to spy on US citizenry to protect American democracy however. The Federal Bureau of Investigations (FBI) routinely tracked citizens and foreign nationals, and monitored them with widespread wiretapping for subversive activities related to Communism (Church Report, 1976; Theoharis, 1981, 2011). These examples show how despite American concerns for human rights, democracy, and the individual, it has been willing to sacrifice the liberties of a few to protect the many when it feels its security is being threatened.

On the surface, US and EU privacy identities and their perceptions of terrorist threats seem rife with incompatibilities. However, European encounters with political violence from nationalist and left-wing groups in the post-war era demonstrated that European states were just as committed to national security, but instead of approaching the problem from a foreign policy perspective, terrorism was criminalized in national laws which place police work at the center of CT efforts. Europeans had experience with both near enemy and far enemy terrorism well before 9/11, and their approaches demonstrate the viability of success through methodologies different from US perspectives, and also room for transatlantic accommodation.

Spain suffered under the Basque Fatherland and Freedom organization, a minority that desired independence and was brutally repressed under Franco's fascist regime until Spain transitioned into a democracy in the late 1970s. The Spanish constitution mentions political violence, provides lawyers and habeas corpus to suspects, and protects them from torture. A central national court in Madrid handles these cases, the *Audiencia Nacional*, and there are allowances for those who cooperate or renounce their connections to violence. The police may violate the right to privacy "if it is proved to be necessary by exceptional or urgent reasons," but this requires an order from the Director of State Security through a judge on the national court (TTSRL Spain, 2008).

Until the 1980s, France distinguished domestic from foreign threats and handled left-wing organizations and separatists with special courts and policing. During the Algerian War, it attempted to use punch cards to identify and monitor migrant workers believed to have ties to separatists, a practice that was banned for civilians but acceptable for Algerians (MacMaster, 2010). For many foreign groups, France followed a "sanctuary doctrine" by allowing its territories to be safe haven in exchange for immunity from attacks.

The sanctuary doctrine proved to be disastrous however, and France soon became the target of Middle Eastern and Islamic separatists in the 1980s. This necessitated a reconceptualization of its CT methods and goals, which resulted in the lengthening of detention times to prevent flight, and legislation, the 1986 September 9th Act, that expanded intelligence gathering and accomplice evidence. As in Spain, a special court in Paris tries all terrorism cases (Wattellier, 2004; TTSRL France, 2008). Unsurprisingly, the French were instrumental in facilitating data sharing through the TREVI system (1976-1988) which coordinated police cooperation among the European states to combat crime, including terrorism, and set up informal networks for data sharing and other multilateral agreements, which eventually formed the core of Europol, the EU criminal intelligence agency (a 2nd pillar institution) in the 1990s (CODEXTER, 2006; Bunyan, 1993).

Germany's approach to CT placed the "security forces of the state…under firm parliamentary control" which meant that surveillance was anchored in human rights but also allowed for proactive police work and the use of high-tech data collection and storage to prevent terrorism on the home front (Katzenstein, 2002). *Apsis*, a computer system that collected and analyzed data on potential suspects was estimated to include nearly 5% of the German population (Beckman, 2007; Flaherty, 1992).

However, Germany's experiences were not limited to near enemy groups. The Red Army Faction had ties to the Palestinian Liberation Organization (PLO) and hijacked a Lufthansa plane in 1976 demanding the release of RAF leaders from German prisons. The PLO killed members of the Israeli Olympic team during the 1970 Munich Games. According to Katzenstein (2002, 2003), the internationalization of Germany's threats created a cultural consciousness and consequentially government practices that rooted CT in criminal law, which was significantly expanded to target leftists, but did have a multilateral dimension with a dependence allied coordination within Europe and with the US (TTSRL Germany, 2008).

The role of law in protecting the human rights of privacy in European CT operations then is multi-leveled. Though national security policies remained independent, the ECHR declares that individuals have the right to "liberty and security of person" and can only be deprived of that right under certain circumstances, which does not include suspected terrorism. An individual can sue the state for compensation in criminal investigations involving violations of their right to privacy (Wattellier, 2004).

Still, there is no cohesive terrorism policy within the EU due to the various types of threats encountered by each state in its history. This also explains why it has been difficult to apply the privacy and data protection provisions legislated under the 1st pillar in cases where 2nd and 3rd pillar issues are involved because protections for 1st pillar data are more restrictive than national security and police officials would like (Bignami, 2007).

The Cold War similarly shaped US ideological perceptions about the world and itself, and having little experience with domestic terrorism, far enemy attacks necessitated the use of sanctions and military action against states that supported attacks against US targets and civilians abroad like Libya (Collins, 2004). Many of the practices – subjugating civil rights in favor of national security, have held constant after 9/11. The US possessed weaker legal protections for individual privacy, which allows law enforcement and government entities more leeway in domestic surveillance and intelligence gathering. The American tradition of secret surveillance was extended by PATRIOT Act after the 9/11 attacks. The Act increased the government's powers in domestic surveillance including individual records held by third parties, searches of private property without prior notification, and the expansion of foreign intelligence collections (ACLU, 2010).

AN (INTER)MESHING OF IDENTITIES AND SECURITY INTERESTS?

The spread of international communications technologies and the transnationalization of political violence put the US and EU privacy identities on a collision course, however both share a desire to protect themselves against terrorist attacks and so there are (and must be) avenues for cooperation. In fact, we have already seen evidence that suggests a (very) slow evolution of melding among transatlantic privacy identities in the last decade.

The EU's pillar structure divided integration into three areas even as these issues overlapped. However, the pillars also allowed for differences in the security cultures and historical experiences held by each European state, which is one reason why the 2nd and 3rd pillars are the least developed in the EU. The EU has not created a Common Foreign and Security Policy (CFSP) and so national perceptions of terrorist threats and the laws that govern them still pervade both intra-EU and transatlantic CT cooperation. Until the pillars are united, the lack of cohesion in security and police policies will enable US to influence, and in many cases circumvent, the EU's privacy and data protections when matters of terrorism are involved. This is however, an opportunity for each side's views on privacy and security to influence the other. Two examples in particular demonstrate how US and EU have influenced each other's data protection practices and hold implications for the future of transatlantic data sharing for counter-terrorism cooperation.

First, in 1995 the passage of 95/46/EC threatened to halt data flows from the EU to the US, but Article 25(1) provided a loophole and allowed the transfer of EU citizen's data to third parties only if that state provided "adequate protections" deemed acceptable by the European Commission's review. What was adequate was left up to the Commission's discretion though, and this ambiguity produced the 2000 Safe Harbor arrangement.

Safe Harbor allowed American companies regulated under the Federal Trade Commission (FTC) or Department of Transportation (DoT) to voluntarily submit to yearly certification by the US Commerce Department to assure that their procedures comply with 95/46/EC's standards. Companies have to either "(1) join a self-regulatory privacy program that adhered to the U.S.-EU Safe Harbor Framework's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the U.S.-EU Safe Harbor Framework." With seven principles for certification based on EU standards, Safe Harbor represented a compromise of the US and EU data protection and privacy identities that satisfied neither side. The agreement communicated EU standards beyond its borders, but depended heavily on the US private sector for enforcement and compliance with no governmental oversight (Kobrin, 2004; Sousa de Jesus, 2004).

However, in January 2012 the European Commission introduced plans to reform the Directive and create a single set of rules enforced by a national data protection authority in each state. In addition to having the right to consent, to access data and be able to transfer data, citizens will also be entitled to "be forgotten" meaning that private corporations and governments

would have limitations on holding data on individuals which included deleting their presence in their data systems. (European Commission, 2012).

There is evidence to suggest that the EU's crackdown on the consumer use of private information has begun to influence the American government's attitudes about the market regulation of data (*The Economist*, 2012). The American public has been calling for more protections of their privacy on social networking sites much in the same vein as Europeans enjoy. A month after the Commission published its reforms, the White House released a proposal for a Consumer Privacy Bill of Rights that included provisions for the fair use of information, transparency, security of data, and the ability to control online tracking (White House, 2012).

Second, directly pertaining to CT cooperation, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) case of 2006-2011 illustrated the connections among privacy and security and how the US could take advantage of the ambiguities in the EU's pillar structure to acquire data. The episode also highlighted areas where the EU could strengthen its data protection framework and bring the US more into line with its privacy rights-based perspective.

SWIFT, a Belgian-based consortium of banks that operates one of the largest financial transfer systems in the world, was subpoenaed for information on individuals with suspected ties to the 9/11 attacks under the provisions of the USPATRIOT Act, which allowed US agencies to obtain financial information in the pursuit of terrorist suspects. Operating within US borders, the Society complied, but as some of the subjects were EU citizens 1st pillar privacy protections were in play. The EU demands that clients be informed their transfers may be subject to scrutiny by American authorities, and it limits the duration that the data can be held by authorities. SWIFT's compliance violated European laws, but was not punished for its role in part because 95/46/EC did not cover data pertaining to security issues, even as the Society's business was engaged in public and private financial services, which clearly fell under the 1st pillar. Finally in 2010, the allies negotiated SWIFT II, which created a US Terrorist Financing Tracking Program (TFTP) and outlined specific conditions and procedures for financial data collection, storage, and sharing to accommodate the discrepancies between US and EU laws. The agreement represented a compromise of both US and European concerns, with a restrictive definition of terrorism that withheld internal Eurozone financial data from the agreement, the installation of an EU scrutinizer, and stricter provisions for the right to be

informed, redress, and right of access. However, Europol's purpose is to aid in the coordination of the member state's criminal investigative and police services and is not a judicial authority, which was necessary for legal oversight (Ripoll Servent and MacKenzie, 2011). Critics surmised that it would transfer data to US authorities without proper legal considerations because of its shared interests, and since Europol can also request data from the US to use in its own investigations it was unlikely to challenge US wishes. Later reviews found that many of the US requests did not provide adequate justification for data access, or were requested orally and without documentation, and yet they were approved (Kierkegaard, 2011; de Goede, 2012). The continuance of bulk transfers of data was another cause for concern, but its continued inclusion in the agreement was due to the "technical" inability to conduct more targeted searches.

Although the SWIFT case seemed to demonstrate Europe's willingness to favor security over privacy, it would be an error to underestimate the strength of the EU's ability to affect the future of transatlantic data policy. Wielding the power of data control is a gradual process, but the EU has been promoting a global standard with each effort (de Goede, 2012; Wade, 2010). The Commission's 2012 reforms will change US-EU data sharing (including Safe Harbor) and gradually move transatlantic data protection towards the European model, if the EU adequately enforces it. The timing of the proposal is important as they will likely affect the renegotiation of the SWIFT agreement which is set to expire in 2015, and the creation of an EU-based TFTP that will have to adhere to European privacy protections. SWIFT undoubtedly provided the impetus to reexamine data protection and privacy issues. And if the EU acts on the Commission's proposals, it will require some intra-EU discussions to bridge the connections between 1st and 3rd pillars and close institutional loopholes that the US has been able to exploit.

CONCLUDING REMARKS

Globalization has spurred a technological and communications revolution, and constructivism demonstrates how social interactions and historical experiences with violence have affected the formation of European and US privacy identities which hold implications for CT practices. The expansion of the global economy has heightened the importance of data sharing in interstate relations and as governments attempt to track networks of violence

they will encounter national legal barriers surrounding cultural ideas and attitudes about privacy that affect their ability to obtain and use data.

There are of course many factors that have influenced US and EU views on privacy and data protection and this article does not pretend to include them all, but it does try to put the development of privacy rights and data protection initiatives on both sides of the Atlantic in a social perspective so that we may postulate how these individual identities will someday create a new transatlantic data sharing regime that accommodates both perspectives of the nature of terrorist threats.

Postscript: This article was written before the recent National Security Agency controversy, and I believe it has strengthened this paper's argument. The American public is now more conscious of its privacy rights to demand reforms. And, these revelations give the EU further incentives to strengthen its data protection laws, which will enable Europe to have a great impact on the future of transatlantic CT operations.

REFERENCES

Allen, Michael. "Stranger than Science Fiction. Edwin Black, IBM, and the Holocaust." *Technology & Culture* 43 (2002): 150-154.

American Civil Liberties Union (ACLU) "Surveillance Under the USA PATRIOT Act. http://www.aclu.org/national-security/surveillance-under-usa-patriot-act (accessed 12 June 2012).

Baldwin, David, ed. *Neorealism and Neoliberalism. The Contemporary Debate*. Cambridge, 1993.

Beckman, James. *Comparative Legal Approaches to Homeland Security and Anti-Terrorism* (Ashgate, 2007).

Bennett, Colin J. and Charles Raab. *The Governance of Privacy*. Ashgate, 2003.

Bignami, Francesca. "Privacy and Law Enforcement in the European Union: The Data Retention Directive." *Chicago Journal of International Law* 8 (2007): 233-255.

Bunyan, Tony. *Trevi, Europol and the European State.* Statewatch.org (1993). http://www.statewatch.org/news/handbook-trevi.pdf (accessed 2 September 2012).

Buzan, Barry. "New Patterns of Global Security in the Twenty-First Century," *International Affairs* 67 (2001): 431-451.

Cannataci, J. "Privacy, Technology Law and Religions Across Cultures." *Journal of Law and Technology* 1 (2009). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/cannataci/ (accessed 20 September 2012).

Center for Democracy and Technology. "Existing Federal Privacy Laws." https://www.cdt.org/privacy/guide/protect/laws.php (accessed 10 September 2012).

Church Committee, Intelligence Activities and the Rights of Americans: 1976 US Senate Report on Illegal Wiretaps and Domestic Spying by the FBI, CIA and NSA.

Collins, Stephen. "Dissuading State Support of Terrorism: Strikes or Sanctions? *Studies in Conflict & Terrorism* (2004): 1-18.

Committee of Experts on Terrorism (CODEXTER) Council of Europe. "Profiles on Counter-Terrorist Capacity, France." June 2006. http://www.coe.int/t/dlapil/codexter/country_profiles_en.asp (accessed 15 September 2012).

Coors, Corinna. "Headwind from Europe: The New Position of the German courts on Personality Rights after the Judgment of the European Court of Human Rights." *German Law Journal* 11 (2010): 527-537.

The Economist, "Private Data, Public Rules." 28 January 2012.

European Commission. "Commission proposes a comprehensive reform of the data protection rules." 25 January 2012 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_ en.htm (accessed 15 June 2012).

Firat, Gamze. *A Common Counter-Terrorism Strategy in the European Union? How Member States' Ideas, Norms and Identities Matter*. MA Thesis. Lund University, Department of Political Science (2010).

Flaherty, David. *Protecting Privacy in Surveillance Societies*. University of North Carolina Press, 1992.

de Goede, Marieke, "The SWIFT Affair and the Global Politics of European Security." *Journal of Common Market Studies* 50 (2012): 214-230.

Hart, Jeffrey A. and Sangbae Kim, "Power in the Information Age." In Jose V. Ciprut, ed. *Of Fears and Foes: International Relations in an Evolving Global Political Economy*. Praeger, 2001.

Hoffman, Bruce. *Inside Terrorism*. Columbia, 2006.

———. "Is Europe Soft on Terrorism?" *Foreign Policy* 115 (1999): 62-76.

Hopf, Ted. "The Promise of Constructivism in International Relations Theory". *International Security* 23 (1998): 171-200.

Katzenstein, Peter J. "Same War-Different Views: Germany, Japan and Counterterrorism." *International Organization* 57 (2003): 731-760.

———. "September 11 in Comparative Perspective: The Antiterrorism Campaigns of Germany and Japan." *International Organization* (2002): 45-56.

Keohane, Robert O. ed. *Neorealism and Its Critics*. Cambridge, 1986.

Kierkegaard Sylvia. "US War on Terror EU SWIFT(ly) Signs Blank Cheque on EU Data." *Computer Law & Security Review* 27 (2011): 451-464.

Kobrin, S. "Safe Harbors are Hard to Find: The Transatlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance." *Review of International Studies* 20 (2004): 111-131.

van de Linde, Erik, Kevin O'Brien (et al.) "Quick scan of post 9/11 National Counter-Terrorism Policymaking and Implementation in Selected Countries." *RAND Europe*. May 2002.

Luebke, David Martin, and Sybil Milton. "Locating the Victim: An Overview of Census-Taking, Tabulation Technology, and Persecution in Nazi Germany." *IEEE Annals of the History of Computing* 16 (1994): 25-39.

MacMaster, Neil. "Identifying 'Terrorists' in Paris: A Police Experiment with IBM Machines during the Algerian War." *French Politics, Culture & Society* 28 (2010): 23-45.

National Security Archive. "Electronic Surveillance From the Cold War to Al-Qaeda." Briefing Book No. 178. 4 February 2006. http://www.gwu.edu/~nsarchiv/ NSAEBB/NSAEBB178/index.htm (accessed 18 September 2012).

O'Cinneide, Colm, Myriam Hunter-Henin, Jorg Fedtke, "German Law" in J.M. Smits ed. *Encyclopedia of Comparative Law* (Elgar, 2006).

Post, Robert C. "Three Concepts of Privacy." *Yale Law School Faculty Scholarship Series*. Paper 185. http://digitalcommons.law.yale.edu/fss_papers/185

Prosser, W. "Privacy". *California Law Review* 48.3 (1960): 383-423.
Regan, Priscilla M. "Global Privacy Issues." *The International Studies Encyclopedia* 2010.
Ripoll Servent, Ariadna and Alex MacKenzie, "Is the EP Still a Data Protection Champion? The Case of SWIFT." *Perspectives on European Politics and Society* 12 (2011): 390-406.
Ruggie, John G. "What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge." *International Organization* 52 (1998): 855-885.
Schoeman, Ferdinand. *Privacy and Social Freedom.* Cambridge, 1992.
Sedgwick, Mark. "Inspiration and the Origins of Global Waves of Terrorism." *Studies in Conflict and Terrorism* (2007): 97-112.
Seltzer, William. "Population Statistics, the Holocaust, and the Nuremberg Trials." *Population and Development Review* 24.3 (1998): 511-552.
Seltzer, William and Margo Anderson. *Census Confidentiality under the Second War Powers Act (1942-1947).* Paper prepared for the Population Association of America Annual Meeting. 29-31 March 2007. https://pantherfile.uwm.edu/margo/public/Confidentiality/Seltzer-Anderson PAA2007paper3-12-2007.doc (accessed 18 September 2012).
Shapiro, Jeremy and Daniel Byman. "Bridging the Transatlantic Counterterrorism Gap." *The Washington Quarterly* 29 (2006): 33-50.
Simmel, A. "Privacy." In D.L.Sills (ed.) *International Encyclopedia of the Social Sciences* 12. (1968): 480-487.
Sorkin, David. "Wilhelm von Humboldt: The Theory and Practice of Self-Formation (Bildung), 1791-1810." *Journal of the History of Ideas* 44 (1983): 55-73.
Strange, Susan. "Finance, Information and Power." *Review of International Studies* 16 (1990), 259-274.
Theoharis, Athan. "FBI Surveillance During the Cold War Years: A Constitutional Crisis." The Public Historian 3 (1981): 4-14.
———. *Abuse of Power: How Cold War Surveillance and Secrecy Shaped the Response to 9/11*. Temple University Press, 2011.
Transnational Terrorism, Security and the Rule of Law (TTSRL) Case Study: France. 28 October 2008.
http://www.transnationalterrorism.eu/tekst/publications/France%20case%20study%20(WP%206%20Del%2012b).pdf (accessed 15 September 2012)
———. Case Study: Germany. 20 November 2008. http://www.transnationalterrorism.eu/tekst/publications/Germany%20case%20study%20(WP%206%20Del%2012b).pdf (accessed 15 September 2012).
———. Case Study: Spain. The Ethical Justness of Counter-Terrorism Measures. 27 October 2008.http://www.transnationalterrorism.eu/tekst/publications/Spain%20case%20study%20 (WP%206%20Del%2012b).pdf (accessed 15 September 2012).
Wade, Ariel. " A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty." *George Washington International Law Review* 659 (2010): 1-15.
Waltz, Kenneth. *Man, the State, and War*. New York, 1959.
———. *Theory of International Politics.* Addison-Wesley, 1979.
Warren, Samuel and Louis Brandeis, "The Right to Privacy." *Harvard Law Review* 4 (December 1890).
Wattellier, Jeremie. "Comparative Legal Responses to Terrorism: Lessons from Europe." *Hastings International and Comparative Law Review* 27 (2004): 1-21.
Wendt, Alexander. "Anarchy is what states make of it: the social construction of power politics." *International Organization* 46 (1992): 391-425.
White House Press Secretary, "Privacy Bill of Rights" 23 February 2012
http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights (accessed 15 June 2012).

Whitman, James Q. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale Law School Faculty Scholarship Series*. Paper 649. http://digitalcommons.law.yale.edu/fss_papers/649 (accessed 10 August 2012)

PRZEMOC, PRAWO I KULTURA – SPOŁECZNA KONSTRUKCJA AMERYKAŃKIEJ I EUROPEJSKIEJ OCHRONY TOŻSAMOŚCI I TRANSATLANTYCKA WSPÓŁPRACA PRZECIW TERRORYZMOWI

S t r e s z c z e n i e

Konstruktywizm społeczny, wpływ idei, doświadczenie historyczne i rozwój kultury w procesach i instytucjach wyjaśniają, jak poprzez historyczne akty przemocy ukształtowało się amerykańskie i europejskie rozumienie prywatności – przekonanie o konieczności ochrony danych osobowych. Ponieważ udostępnianie danych ponad granice stało się ważnym elementem walki z terroryzmem, różnice w transatlantyckim rozumieniu prywatności wpływają na współpracę w „walce z terrorem".

Europejskie doświadczenia w zarządzaniu państwami, radzenie sobie z lewicowym i nacjonalistycznym terroryzmem (bliskość zagrożenia ze strony wroga) podczas II wojny światowej i Zimnej Wojny wytworzyły kulturalną świadomość, która ukształtowała europejskie rozumienie prywatności jako podstawowego prawa człowieka. Ochrona danych osobowych przysługuje każdej osobie jako zabezpieczenie przed wtargnięciem organów państwa lub innych postronnych osób w jej życie prywatne. Metody europejskiej walki z terroryzmem rozwinęły się w ramach prawa karnego, które wymagało, by urzędy uszanowały tożsamość narodową i ochronę danych osobowych w trakcie śledztwa.

Stany Zjednoczone nie doznały przemocy politycznej w czasie II wojny światowej i Zimnej Wojny, ale były często celem zewnętrznych ataków terrorystycznych (ze strony „dalekiego wroga"). W efekcie amerykańska walka z terroryzmem polegała na interwencjach militarnych, tajnych akcjach i sankcjach wobec państw, które wspierały te grupy. Zezwalano również na tajne zbieranie danych i nadzór nad swoimi obywatelami i cudzoziemcami. Amerykańskie rozumienie prywatności jest oparte na własności i chroni dane posiadane przez właściciela, niezależnie od tego, kto nim jest. Wobec tego ustawodawstwo selektywnie regulowało użycie danych.

Te rozbieżności w rozumieniu prywatności są ważne dla współczesnej współpracy w walce z terroryzmem, ponieważ technologie informatyczne i zagrożenia przekraczają granice niezależnych państw, powodując coraz większe ujednolicenie i niwelację rozbieżności w rozumieniu prywatności, systemów prawnych i interesów związanych z bezpieczeństwem przez poszczególne narody. Konstruktywizm wyjaśnia powstawanie i oddziaływanie instytucji i procedur w danym społeczeństwie i w relacjach między społeczeństwami. W związku z tym artykuł, wskazując na doniosłość bezpieczeństwa, pokazuje rozwój w ostatniej dekadzie transatlantyckiej wymiany danych, która objęła zarówno amerykańskie, jak i europejskie rozumienie prywatności.

Przełożył Krzysztof Modras

VIOLENCE, LAW AND CULTURE: THE SOCIAL CONSTRUCTION OF US AND EUROPEAN PRIVACY IDENTITIES AND TRANSATLANTIC COUNTER-TERRORISM COOPERATION

S u m m a r y

Social constructivism, the influence of ideas, historical experience and culture on processes and institutions, explains how US and EU privacy identities—beliefs about the protection of an individuals' data, have been shaped by historical episodes of violence. As sharing data across borders has become an important component of counter-terrorism (CT) operations, the differences among transatlantic privacy identities will affect cooperation in the "War on Terror."

European experiences with state-led, left-wing, and nationalist terrorism (near enemy threats) during the Second World War and Cold War eras created a cultural consciousness that framed the EU's privacy identity as a fundamental human right where data ownership is vested in the individual to protect intrusions from the states or private citizens. European counter-terrorism (CT) strategies developed within criminal law, which required officials to take notice of national privacy and data protection protections in their investigations.

The US did not encounter political violence during World War II or the Cold War, but was frequently the target of terrorism aboard (far enemy). As a result, US CT relied on military intervention, covert action, and sanctions against states who supported these groups, while allowing covert data collection and surveillance on its citizenry and foreign nationals. The American privacy identity is property based, and protects data in the possession of the holder, no matter what entity this might be, so legislation has selectively regulated data usages.

The variances in privacy identities are important to contemporary CT cooperation because information technologies and threats transcend sovereign borders causing national privacy identities, legal systems, and security interests to increasingly overlap and clash. However, as constructivism shows how institutions and procedures have been the result of interactions within societies and among societies, the last decade has shown how transatlantic data sharing has evolved to encompass both US and EU privacy and security values.

Summarised by Michelle Frasher

Key words: social constructivism, culture, law, terrorism, privacy, data protection, Europe, United States.

Słowa kluczowe: konstruktywizm społeczny, kultura, prawo, prywatność, ochrona danych, Europa, Stany Zjednoczone.