HASTINGS INTERNATIONAL AND COMPARATIVE LAW *Review*

Volume 36, No. 1 — WINTER 2013

HASTINGS INTERNATIONAL AND COMPARATIVE LAW *Review*

VOL. 36 **Winter 2013** **NO. 1**

Table of Contents

ARTICLES

On June 24, 2011, the Court of Military Commission Review (CMCR) released its decision in the case of *U.S. v. Hamdan*, holding that material support for terrorism (MST) constitutes a law of war violation. The Court of Appeals for the D.C. Circuit granted certiorari and heard oral arguments in the case on May 3, 2012. The court released its decision on October 16, 2012, as this article was going to the publisher. This article argues that the charge of MST is not a violation of the law of war, and that is the conclusion ultimately reached by the D.C. Circuit.

This article contends that MST can be viewed as the consistent logical continuation of the Bush Doctrine, a sweeping pronouncement that the U.S. will make no distinction between those who aid terrorists and the terrorists themselves. Both MST and the Bush Doctrine seek to impose liability on a third party, provided that party possesses a "permissive" *mens rea*, and performs some act falling within the broad ambit of material support, regardless of whether the assistance intended to further a terrorist act.

The Obama Administration has largely accepted the

theoretical underpinnings of the Bush Doctrine while endorsing a bifurcated approach to military commissions. Despite a lack of bipartisan support for bifurcation, after two acts of Congress, a Supreme Court decision and an executive review, the military commissions system is at long last a fair and transparent forum for the administration of justice. Nevertheless, continuing to charge suspected terrorists with MST before military commissions not only threatens hard-won convictions, but has renewed questions about the system's legitimacy.

The CMCR's holding that MST constitutes a war crime rested on a subtle, yet fatal error. In its decision, the court conflated mere criminal acts with war crimes. Notwithstanding the CMCR's holding, the charge of MST cannot be said to constitute a violation of the laws of war, and military commissions have no jurisdiction over the charge. As military prosecutors continue to level the charge, they compromise the commissions' credibility and defer total redemption.

This article describes both e-discovery in the United States and the German Federal Data Protection Act, the Bundesdatenschutzgesetz (BDSG). It details the conflicting demands of those institutions in the event of litigation, as well as the consequences for a company caught between them. Namely, e-discovery often requires the disclosure of vast amounts of electronically stored information held by a company, while the BDSG prohibits the disclosure of personal information outside of specific exceptions. Failure to disclose the data could result in significant sanctions in the U.S., while disclosing data can lead to large fines and constitutes a criminal offense in Germany.

Next, the article describes two ways to prevent discovery that conflicts with the BDSG: protective orders and the *Aerospatiale* test. A protective order requires a showing of "good cause," and the BDSG can satisfy that requirement. The Supreme Court's *Aerospatiale* test is used to determine when comity prohibits use of FRCP discovery. Because the

Aerospatiale test references the Hague Evidence Convention as an alternative to FRCP discovery, the article then describes the Convention and how it can be used.

Finally, the authors present some advice for companies to avoid the e-discovery/BDSG conflict. This advice includes storing personal information separately from nonpersonal information, avoiding transferring information collected elsewhere into Germany, and cooperating with the opposing party and the court during the discovery process.

On July 2, 2012, Verizon filed a brief with the United States Court of Appeals, District of Columbia Circuit, stating that the open-network, antidiscrimination rules adopted by the Federal Communications Commission "violate[d] the First Amendment by stripping [Verizon] of control over the transmission of speech on [its] network." Verizon argued that its broadband network is its "microphone" and its "newspaper," essentially claiming the online communications of some 200 million Americans as its own.

This article first describes how the United States First Amendment and communications law have evolved to a point where Verizon's argument is plausible. It then compares our own network-speech jurisprudence with that of a different constitutional culture. The First Amendment, while understood as a "free speech" protection, is frequently just the opposite – either missing in action, or applied to lessen the amount of speech, information, and opinion available to the public. One reason for this is that courts have typically focused on the "government shall make no law" language rather than the "freedom of speech" phrase at the end of the First Amendment.

The German post-war constitution (the *Grundgesetz* or Basic Law), by contrast, was built on the ashes of a fascist dictatorship that had misused mass communications, and was structured to make a similar catastrophe as unlikely as possible in the future. Its speech article (Article 5) guarantees the

"institutional freedom" of broadcasting and the press, and protects speech and information transfer as dynamic processes. The German Constitutional Court has interpreted Article 5 to require the state to safeguard the opinion and information-transfer functions of broadcast media in particular, and of "individual and public opinion-building" in general, as necessary conditions for democracy.

NOTES

Large, multinational corporations today preserve vast quantities of electronic data out of fear that they will suffer sanctions under the Federal Rules of Civil Procedure for destroying evidence that could be relevant to ongoing or pending litigation. But, as U.S. companies hoard data, European regulators are stepping up enforcement of privacy laws that require the systematic elimination of data that identifies individuals without their consent. These laws, such as EU Directive 95/46, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, are arguably far-reaching and may affect data relating to persons with only minimal contacts in the European Union. In some cases, current and proposed laws could implicate data preserved in the United States that has no connection to any EU resident. Litigants in U.S. courts know well that American judges can and do order *production* of evidence despite foreign privacy laws forbidding it – creating a Hobson's choice between sanctions here for non-compliance with discovery orders or sanctions abroad for violation of the privacy law. But, the ways in which *preservation* alone can violate non-U.S. data protection laws is less well-known. If current trends continue, however, the over-preservation practices of multinational corporations could come under the scrutiny of European regulators who are increasingly empowered to enforce potentially broadly applicable data protection laws.

The Department of Justice and the Securities and Exchange Commission aggressively pursue and punish individuals and companies who bribe or attempt to bribe foreign officials in other countries pursuant to the Foreign Corrupt Practices Act of 1977 (FCPA). However, the FCPA as it is currently interpreted by the Department of Justice has been the object of growing criticism. The United States Chamber of Commerce has argued that good faith efforts to comply with the law are often unsuccessful and that statutory amendments are necessary to "secure clarity" with respect to enforcement policy. A year ago, the Department of Justice responded to this criticism by publicly commiting to release guidance on the FCPA's criminal and civil enforcement provisions. Commentators argue that this guidance, if the Department ever issues it, is not likely to respond to the criticims of scholars and practitioners who oppose the current enforcement policy altogether. This Note finds that statutory amendments are necessary to require the DOJ to take notice of, and respond in a meaningful way to, the legitimate criticism of its current enforcement policy.

This Note begins with an introduction to the text of the antibribery provisions, followed by a summary of two of the COC's key criticisms of the FCPA as currently interpreted by the DOJ. It then examines the procedural law governing the DOJ's enforcement policy formulation to demonstrate that the Department has consistently chosen the least transparent means to formulate its enforcement policy. Finally, the Note concludes by briefly comparing legislative and administrative developments in the United Kingdom surrounding that country's UK Bribery Act 2010 as a potential procedural benchmark for Congress to better guide the DOJ procedurally in formulating its enforcement policy.