In den USA hingegen habe traditionell nicht die Technik, sondern der Schutzgegenstand selbst im Mittelpunkt der Regelungen gestanden, was dazu beigetragen habe, dass gesetzliche Regelungen weit mehr auf das Verhältnis zwischen Staat und Bürger beschränkt geblieben seien.

Gleichwohl habe man auch in den USA die Gefahren für den Einzelnen nicht übersehen. Man reagiere dort aber deutlich anders und versuche, neuen technischen Entwicklungen nicht vorrangig mit dem europäisch geprägten „Primat der Verrechtlichung", sondern mit administrativen Regelungen für einzelne Sachverhalte („policies") zu begegnen, wodurch eine deutlich schnellere Entwicklung möglich sei als im Rahmen von langwierigen Gesetzesverfahren.

Neben kulturell bedingten Aspekten trete im Bereich der internationalen Rechtssetzung auf Seiten der USA ein institutioneller Grund für die dort vorzufindende Scheu vor einer weiteren Verrechtlichung. Dieser liege darin, dass die außenpolitische Kompetenz im Wesentlichen beim Präsidenten, die Rechtssetzungskompetenz aber im Wesentlichen beim Kongress liege. Auch deshalb sei nicht davon auszugehen, dass die USA den europäischen Entwicklungen im Datenschutz folgen würden.

Hieraus schloss *Dr. Stentzel*, dass ein wirksamer Datenschutz auf beiden Seiten des Atlantiks nur dann verwirklicht werden könne, wenn zwei fundamentale Missverständnisse ausgeräumt würden: Auf der einen Seite müsse die EU erkennen, dass das „Recht als solches" nicht einfach in die USA exportiert werden könne, auf der anderen Seite müssten aber auch die USA erkennen, dass die EU ihren Ansatz der Verrechtlichung nicht aufgeben werde.

Für die europäische Seite befürwortete der Referent daher einen Lösungsansatz auf untergesetzlicher Ebene, der durch Elemente der Selbstregulierung ergänzt werden sollte. Hierzu habe die Bundesregierung auch bereits auf europäischer Ebene einen Vorschlag eingebracht, der bereits bestehende Ansätze in dem Verordnungsentwurf noch ausbauen solle. Dieser sehe vor, dass Anreize für Unternehmen geschaffen würden, unter Beteiligung der Datenschutzbehörden und anderer Interessengruppen Verhaltenskodizes zu entwerfen, welche anschließend dem europäischen Datenschutzausschuss vorgelegt werden müssten. Hinsichtlich der genauen Ausgestaltung von Verfahren und Rechtsfolgen einer solchen Selbstregulierung sei allerdings noch einige Arbeit zu leisten.

3. Diskussion

In der Diskussion begrüßte *Dr. Arnd Haller* (Google Deutschland) die Vorschläge zur verstärkten Selbstregulierung von *Dr. Stentzel* und ergänzte, dass Datenschutzbehörden derzeit keine Anreize für eine Kompromisslösung hätten, sondern vielmehr tendenziell auf Maximalforderungen beharren könnten.

Anschließend warf *Dr. Haller* das Problem eines „Rechts auf Vergessen" auf und verwies auf einen laufenden Fall vor dem EuGH, in dem mit diesem Recht ein Anspruch gegen Google begründet werde, bestimmte Suchergebnisse zu löschen. Er wies dabei auf die Gefahren für die Meinungsfreiheit hin und kritisierte, dass bei Bejahen eines solchen Anspruchs das „Primat des Datenschutzrechts" andere rechtliche Regelungen untergrabe.

Dr. Stentzel erläuterte daraufhin die differenziert geführten Diskussionen auf europäischer Ebene und wies am Beispiel eines ausgeschütteten Federkissens darauf hin, dass rein faktisch ein Recht auf Vergessen kaum durchsetzbar wäre. Jedenfalls leichter durchzusetzen sei ein Löschungsrecht in Bezug auf genau beschriebene Typen von Daten, etwa solche, die von dem Betroffenen selbst in das Internet gestellt wurden. Er gab aber auch zu bedenken, dass man vorsichtig sein müsse, über den Umweg des Datenschutzes als originär öffentliches Recht zu großen Einfluss auf eigentlich zivilrechtliche Fragestellungen zu nehmen.

*Beate Parra**

The Legal Profession in Times of Cloud Computing and Social Media

Ethics and the Use of Technology by Lawyers on October 9, 2013 at Deutsches Haus in New York

On October 9, 2013, Fordham Law School, American Friends of Bucerius, the German American Chamber of Commerce and the German-American Lawyers Association (DAJV) jointly sponsored a moderated panel discussion at Deutsches Haus in New York City. The timely and highly relevant topic of discussion was the ethical and practical impact that cloud computing, social media and other new technologies have on practicing lawyers and the legal profession. Approximately 40 participants attended.

Eileen Goltz attended as the representative for the German Consulate in New York.

Susanne Gellert, LL.M., Head of the Legal Department of the German American Chamber of Commerce in New York delivered brief welcoming remarks. Dr. *Nina Schmidt*, President of the American Friends of Bucerius in New York and Director of Strategic Planning and Business Development ZEIT-Stiftung Eberlin und Gerd Bucerius in Hamburg noted that this event constitutes the first Continued Legal Education event in this format. She introduced the moderator, *Joel Cohen*, Esquire, noting that Mr. *Cohen* is the founder and curator at Talks On Law, a law and media company focused on cutting-edge legal thought and practice. Prior to TOL, Mr. *Cohen* practiced corporate law at Skadden, Arps where his practice focused on cross-border transactions and mergers and acquisitions.

Mr. Cohen (*JC*) introduced the panel members.

Prof. Joel Reidenberg is a law professor at Fordham Law School and a founding Academic Director of the Center on Law and Information Policy at Fordham Law School. He has

* Executive Director & Assistant General Counsel Mitsubishi UFJ Securities (USA), Inc.

been published widely in the U.S. and Europe, and is the co-author of three leading books and monographs on international data privacy. Prof. *Reidenberg* testified before the U.S. Congress on data privacy issues and is a consultant to the Federal Trade Commission and the European Commission.

Harriet Pearson, Esquire, is a partner at Washington office of Hogan Lovells. She has been referred to as the "first lady of privacy" and "queen of social media." After a long tenure as the Chief Privacy Officer at IBM, she currently co-chairs the Georgetown University Cybersecurity Law Institute and serves on the ABA President's Talk Force on Cybersecurity.

Timothy P. Harkness, Esquire, is a litigator handling complex litigations at Freshfields Bruckhaus Deringer. He played prominent roles in major cases involving international financial service and accounting firms in securities fraud cases, hedge fund-related litigation and commercial disputes. He is actively involved in alumni affairs at Yale University.

JC opened the session noting that the panel would discuss the following three topics: 1) Social Media; 2) Cloud Computing; and 3) Law and Technology.

By way of introduction, he noted that there is a wide range of applications, developers, users, usages and experiences across the social media landscape. However, generally speaking, the younger the person, the more familiarity with social media can be expected. *JC* commented that as a profession, lawyers are behind the curve when it comes to social media usage and that judges are even further behind.

Professor Joel R. Reidenberg (*JR*) presented a series of slides on legal issues in connection with technology and social media. *JR* polled the audience by a show of hand as to how many participants were users of Facebook, LinkedIn, Instagram, Twitter, as well as how many participants were familiar with the privacy settings for each social network. *JR* explained that at its most basic, a social network is a website that allows people to sign up and "friend" others. Twitter allows users to publicly comment in 140 characters. *JR* next commented on blogs that allow users to post commentary usually hosted by a third party. He explained that while it is up to the social network to set a privacy policy, users control the individual privacy settings and it is important to be familiar with these settings. *JR* explained that users can be "tagged" both in pictures as well as comments and social networks allow comments to be magnified out. The rise of social media has led to a dramatic growth in data streams which allow third parties to locate users and "geo-tag" them. *JR* noted that using social networks can be for personal use but are increasingly powerful commercial and marketing tools. As a result, the legal and societal implications on personal privacy, transparency and ethics are huge. He noted that the use of social media by employees while on business trips can provide third parties with sensitive information about potential strategic plans. *JR* concluded his presentation noting that particularly for lawyers and judges, social networks can be a legal and ethical minefield, such as when lawyers Google jurors or judges and jurors are "friended." *JR* noted that all social media communications are considered ex parte. He added that at least under New York law, lawyers are allowed to Google jurors but prohibited from "friending" them. Judges in particular should be very judicious in the use of social media. *JR* pointed to the American Bar Association guidelines whereby judges should avoid any use of social media that would present an appearance of favoritism. *JR* mentioned case law in Florida where a judge was disqualified from a case because he was a Facebook friend of the prosecutor in that case. In response to a question from the audience, *JR* pointed out that Facebook and other social media applications lead to small town-type intertwined community relationships. He explained that if a social media connection is such that it may appear that the relationship might be close enough to require a judge's recusal, then the judge is best advised to recuse himself or herself even if the relationship is not truly close.

Timothy P. Harkness (*TH*) echoed *JR*'s comments on social media as an ethical minefield as he related his experiences with social media in his litigation practice. He pointed out that social media plays a part in almost all of his cases and while he does not really have a technical background, he tries to stay as current as possible, including by talking to younger attorneys in his practice group. *TH* stated that the internet is truly a treasure trove of evidence, such as pictures, blatant lies and even confessions. He noted that it is quite astounding that many users keep posting on social networks even after an investigation or litigation has begun and sometimes go so far as to comment on active cases. *JR* pointed to a series of sanction cases where social media statements could be used to impeach in-court testimony by attorneys and witnesses. He cautioned that "friending" a represented party is a violation of the no-contact rule and "friending" someone under false pretenses is not permissible. He described that he conducts social media reviews for all of this cases, i.e. for each potential witness, including his own. He noted that these searches have to be conducted periodically since content changes constantly and recommended saving screen shots with important information. *TH* noted that spoliation is a risk and that a Facebook profile, for instance, is arguably a document that should not be altered or destroyed after the commencement of a case. He referred to a case where a lawyer was sanctioned for telling a client to clean up a Facebook page after receiving a document request. *TH* added that a review of potential jurors via LinkedIn must be carefully thought through since visits to a person's LinkedIn profile leave a record. He added that in this context an additional problem arises due to the fact that research has shown that about one-third of LinkedIn users lie or misrepresent information on their LinkedIn profile. In concluding, he recommended that attorneys stay current on ethical opinions issued by Bar Associations since the area of law is evolving so quickly.

Harriet Pearson (*HP*) addressed the audience stating that every company should have a robust social media policy and recounted her own professional experience with developing and drafting one while working as in in-house attorney at IBM. *HP* described how in 1995, she was asked to help determine whether or not IBM should allow employees to use the internet and in response helped draft a policy on internet usage. In 2005, after she became IBM's Chief Privacy Officer she was approached by a developer who with his colleagues had begun to create a web log (blog). They had created certain rules for blogging and asked for her input and additional advice. Both documents became the basis for IBM's current social media policy. *HP* noted that it is important that the policy be tailored to the company's business strategy, adding that IBM's policy is relatively open and permissive. *HP* highlighted a few potential legal and business risks that should be carefully considered when drafting the policy. For public companies, for instance, tweeting may violate securities regulations. Under the U.S. Securities and Exchange Commission's fair disclosure regulation, known as Reg. FD, public companies may not selectively disclose material non-public information to market professionals or stockholders. *HP* explained that while the SEC has issued guidance indicating that a company may use its website or blog as a FD compliance disclosure tool, disclosures via a tweet or social media posting have not been

deemed sufficiently broad-based to meet the Reg. FD requirement. *HP* pointed out that any disclosure about the company or its employees must be done in a thoughtful manner so as to not accidentally violate Reg. FD. She noted that even employees disclosing information about their travels via blogs, tweets or postings on a social network may provide a competitor with insights as to the company's strategic business expansion, potential transactions or client identification. Issues can also arise when a company tries to restrict employees' blogs, posts or tweets regarding work conditions at a particular employer. The National Labor Relations Act protects the rights of employees to act together to address conditions at work and the federal agency in charge of enforcing the law has extended that protection to certain work-related conversations conducted on social media, such as Facebook and Twitter. A good social media policy should also provide guidance to the Human Resources Department as to how much information they may gather from social networks when recruiting talent. *HP* pointed out that conducting research about a candidate on LinkedIn is acceptable, on Facebook probably as well, but a company may not ask for an employee's Facebook password.

JC next moved on to the second topic of Cloud Computing.

JC first explained that cloud computing is here to stay and can be expected to grow significantly. Amazon, DropBox, Gmail and many others offer cloud computing services to companies and consumers that allow for a less expensive form of data storage. *HP* noted that cloud computing is very simple in principle but will have a hugely profound effect on data storage, ownership, transparency and other ethical and legal issues. *HP* explained that traditionally server-based computing power was either stored on a desktop or locally outsourced to datacenters. In comparison, it is as if computing power now comes out of a faucet and small businesses can tap directly into computing power and buy it as needed which provides for significant innovation and change for consumers and users. *HP* noted that numerous legal issues arise in this context: how will a company know who has access to the information that it has collected from its customers? How is the data secured? Who is given access to the data? Where is the data located? Whose data privacy laws apply when company, customers and cloud computing providers are located in different jurisdictions? What access to the data will governments and law enforcement have? What issues arise if the cloud computing provider experiences a data breach? What if it becomes insolvent?

In response to a question from the audience, *TH* explained that a party can serve a subpoena on a company providing cloud computing services. He noted that companies conduct risk assessments and draft risk matrices based on where data is located. *HP* added that large companies have leverage to heavily negotiate the service contracts with cloud computing service providers eager for business.

JR noted that as a consequence of the disclosures by Edward Snowden of classified details of several top-secret U.S. and British government mass surveillance programs to the press, U.S. companies have lost billions of dollars in cloud computing services. However, according to *JR*, moving the hosting service to Europe will not solve the problem of access to data by governments and law enforcement. *JR* noted that data trails can establish who is communicating with whom. *JR* also explained that metadata can be far more revealing than content data given that individual behaviors can be discerned by tracking metadata patterns. *JR* stated that at its core tension consists of legal access requirements in the U.S. conflicting with data privacy rules in Europe.

In response to a question from the audience inquiring about any statistics about lost, destroyed or illegally accessed data in the clouds, the panel agreed that while there are not readily available statistics, the risk is ever increasing due to more volume, more bad actors (individuals and states) and the proliferation of devices making data breaches more likely. Attorneys and data security experts must perform proper due diligence and risk assessments on cloud service providers. In this context, *JR* suggested to the audience as a homework assignment to ask the Head of IT at their workplace to tell them how many intrusion attempts occurred on any given day. *JR* noted that if the answer is 0, the time may have come to find a new Head of IT.

In response to a another question from the audience as to whether the U.S. is doing enough to protect larger cloud service providers from bad actors, *HP* noted that it is difficult to generalize but in comparison to other locations, the problem is well known and the U.S. is about a decade ahead in thinking about ways to protect assets with national security implications. President Obama issued an executive order create a cybersecurity framework for critical network infrastructure.[1]

JC next guided the conversation to the panel's final topic – law and technology. The panel highlighted the increase in usage and sophistication of smart technology and explained how companies are using that technology to anticipate customers' buying patterns and consumption preferences. *JR* pointed out that lawyers will need to adapt but also think about how we should as a profession respond to the issues of privacy and over-transparency of citizens. *HP* added that for the tech industry the 1990s and early 2000s were optimistic times with very little regulation or government interference. Now the situation is more reminiscent of a digital cold war.

JC concluded the session by summarizing that we live in very interesting times, full of risks and threats on one hand but plenty of opportunities on the other hand.

1 After the event held on October 9, 2013, the National Institute of Standards and Technology (NIST) issued its Preliminary Cybersecurity Framework (the Preliminary Framework) on October 22, 2013. The Preliminary Framework represents the first full draft of the Cybersecurity Framework (the Framework) that President *Obama* ordered NIST to develop in his February 12, 2013, executive order addressing the regulation of critical infrastructure network security.