

Law & Technology of Digital Information Management: Promises, Challenges, and Perspectives

Observations in the Aftermath of an Interdisciplinary Workshop

This report expands on some of the themes explored in an interdisciplinary expert workshop on the Law and Technology of Digital Information Management that was organized by the Research Center for Information Law at the University of St. Gallen (FIR-HSG) in collaboration with the Credit Suisse Group (CSG), Zurich, and was aimed at discussing the organizational, technological, and legal problems associated with the transition from analog/offline to digital/online information management systems in the corporate world. The following text includes some of the key findings of the workshop, but is not intended as a verbatim summary. Instead, it offers a personal memoir of the chairmen of the workshop, Urs Gasser (University of St. Gallen) and Domino Burki (Credit Suisse Group).

The private sector’s transition from the “paper world” to a digitally networked information environment has been accompanied by a number of complex challenges at the intersection of technology, business practices, and the law. These challenges take place at different management levels. At the level of strategic management, for instance, corporations face the challenge of designing coherent records management and data retention policies—as important building blocks of the corporate governance system—vis-à-vis heterogeneous legal requirements, while maintaining efficient commercial operations in data storage. In this context, the workshop participants explored some of the key issues that need to be addressed in document retention policies, such as their interaction with other policies (e.g. data protection policies, web and email policies) as well as substantive issues like ownership of data, responsibility, and security. Focusing on the particularly sensitive issues to be decided at the level of strategic management, the participants put emphasis on two areas.

The first aspect concerns the allocation of control over data within an internationally operating corporation. Most participants agreed with the analysis that custody of data—as opposed to the place of data storage or the physical location of the
servers—is increasingly the decisive factor in cases where stakeholders (e.g. law enforcement authorities; plaintiffs) seek access to information stored in corporate information systems. According to U.S. discovery rules, for instance, custody of data is the essential criterion for obtaining access to data, while the place of data storage and the physical location of the server, respectively, have become less relevant. Against this backdrop, the management may be well advised to consider decentralized information management systems, where data is stored in closed, geographically segmented electronic networks.

The second area of concern discussed at the workshop relates to what one might call the ecology of the corporate information system, i.e., the tension between data retention versus data destruction. On the one hand, laws and regulations require that data processing, including data retention and archiving activities, must not be excessive and therefore require the destruction of dispensable data. On the other hand, destruction bans or litigation holds, usually relatively vague in their scope, force multinational companies to retain such data. An analogous tension between retention and destruction interests also exists with regard to data as potential evidence: On the one side, companies may have an interest in extended data preservation in order to provide evidence in court proceedings—destruction of data, in fact, could even be considered a frustration of evidence—while extensive data retention practices on the other side may motivate extended inquires by third parties or law enforcement authorities.

Although clear-cut safe harbor rules for cases in which data has been destroyed in accordance with a company’s internal data retention policy have not yet been enacted (but are considered in at least some jurisdictions, including the U.S.), the workshop participants agreed on the importance and promise of a systematic, “best practice”-oriented approach to records retention and destruction. A key element of such a systematic approach is software that enables deletion of data and metadata, but allows tracking the responsibility for the decision to delete data.

A corporate policy aimed at structuring the transition from an analog to a digital corporate information environment and regulating digital data management practices, as any other policy, needs to be implemented. The implementation of the data policy decisions taken at the strategic level requires important decisions at the level of operative management where technological, organizational, behavioral and financial elements
interact. The workshop participants explored several areas that deserve special attention by the operative management. One of the key challenges is providing and coordinating the necessary resources to keep pace with the exponential growth of corporate information and to appropriately manage digital records throughout their life-cycle. A second challenge relates to the development and application of intra-organizational enforcement tools and practices aimed at enforcing records management policies and procedures across the enterprise. It has also become clear that it is increasingly important to master the interactions between human decisions and the technology of information management. From a technological viewpoint, for instance, it is possible (as mentioned above) to implement software that is able to retrieve all documents subject to a destruction ban, to mark them and thus to exclude them from destruction. From a behavioral perspective, however, one has to manage the phenomenon that not all documents are labeled correctly (e.g. typos, indexing errors) and, as a consequence, that human decisions are still necessary.

At the center of the digitally networked corporate environment are nearly perfect information systems in which almost all actions are systematically recorded and stored, leading to complete data trails. As the private sector is gathering more and more data on customers, suppliers, competitors, etc., various stakeholders such as potential plaintiffs or law enforcement authorities intensify their efforts to gain access to corporate digital information systems for their respective purposes. The resulting conflict between interests in disclosure of data versus privacy interests (including, among other things, banking secrecy) has not yet been balanced by an advanced legal and regulatory framework, neither at the national nor at the international level. In fact, the possibility of global access to corporate information systems (e.g. law enforcement authorities in one country may require a subsidiary to grant access via electronic network to data “belonging” to the headquarters operating in a different country) are in sharp contrast to the heterogeneous local laws and practices regulating access to data. Against this backdrop, the workshop participants explored two specific questions in greater detail.

First, practical and theoretical problems in cross-border litigation (e.g. considering the Hague Convention) were discussed by analyzing an actual example of a foreign plaintiff who sued a Swiss company before a Swiss court after gaining access to data
from the US subsidiary based on a provision regarding assistance to foreign tribunals, and sought to use the so collected data in the relevant Swiss procedure.

Second, the practical significance of Art. 271 of the Swiss Penal Code (illicit acts on behalf of a foreign State) and Art. 273 Swiss Penal Code (economic espionage) is up for discussion in an environment where data hosted in Switzerland can be accessed from abroad. In fact, anecdotal evidence suggests that local authorities in foreign countries—as well as plaintiffs in civil litigation (eDiscovery)—seek to gain direct electronic access to data in cases where, under a “paper world scenario,” access would usually require compliance with well-balanced legal or administrative assistance procedures. In this area, the workshop participants identified both the need for further in-depth legal research where theory and practice work hand in hand and may lead to policy recommendations as well as a cross-industry approach aimed at raising the awareness of foreign judicial authorities as to the existence of comparatively strict privacy laws in Switzerland.

In conclusion, the workshop participants agreed that multinational corporations, regardless of the products and services they offer, are increasingly also in the IT business in the sense that the design of digital information systems becomes an important management issue that no longer can be left to the discretion of IT departments, but must be understood as an integrative element of corporate governance and strategy that requires the attention of the top management. The need for an advanced "cyber-strategy" was particularly emphasized by Professor Charles Nesson, Harvard Law School. The participants also made specific suggestions as to how to deal proactively with some of the key problems outlined in the previous paragraphs. At the core is the idea to organize abroad an off-the-record workshop, in which representatives of multinational corporations headquartered in Switzerland—using peer-produced hypotheticals and case studies as threads—could further explore in dialogue with foreign judges, government authorities, private sector representatives, and academics the challenges and promises of digital or hybrid enterprise content management systems in a globalized world with its heterogeneous legal frameworks. Alternatively, the participants envisioned a public cross-industry summit in order to further discuss the key issues identified in CSG/FIR workshop.