Ask a RIM Law Expert

This is part of a syndicated column I have created for ARMA chapters. My column is devoted to answering information governance, records management, privacy and related legal questions from Chapter Members or sharing my thoughts on current hot topics. As you read my column, please note that although I am an attorney specializing in these areas of law, these are only my opinions. My opinions should not be construed as legal advice. Kindly consult with an attorney for more formal advice.

This month I have been inundated with questions about the Hilary Clinton personal email account issue, while she was Secretary of State. Following are my responses to some of the questions I have received from media news outlets.

Are personal emails discoverable in court?

Yes. A few courts have already broached this issue. For instance, in Stengart v. Loving Care Agency Inc., Case No. A-3506-08T1 (NJ Sup. Ct, Appellate Div., June 26, 2009), the defense sought production of Stengart's email communications with her attorney, which she had written from the office computer of the very employer she sued. The court ruled that the employee's personal email communications with her attorney, through her work computer, were not discoverable because her employer permitted some personal use of office computers for personal matters. If the employer policy had forbidden personal use of office computers, the outcome could have been very different.

In another case, Lake v. Phoenix (Ariz. Ct. App., No. 07–415, 1/13/09), the court noted that courts in Arizona have distinguished between "public records" and all other records created as a result of government employees' activities. The issue of public records is a close cousin of the discoverable records issue in litigation. In either scenario, the personal email of an employee is not necessarily discoverable or a public record. It all depends on the context of the communication and the jurisdiction where it occurred.

Such context presented itself in O'Neill v. City of Shoreline, 2010 WL 3911347 (Wash. Oct. 7, 2010). There the Supreme Court of Washington held that emails sent to a government official's private email home account were considered subject to Washington's Public Records Act ("PRA"). On September 14, 2006, Diane Hettick, a private citizen, sent an email to Lisa Thwing, a private citizen, containing criticism of the Shoreline City Council ("the Council"). Thwing forwarded that email to herself and then to Shoreline Deputy Mayor Maggie Fimia. The email to Fimia (the Mayor) was unsolicited and was received "at home on her personal computer." However, Fimia took the extraordinary measure of reading the email out loud at a city council meeting. As a result, the Court held that an e-mail sent to a personal home computer, but discussed at a city council meeting, is a "public record" and should have been disclosed in response to a request under Washington's Public Records Act.

How can organizations find out if an executive is using personal email accounts for business? Is it typically after something goes wrong (like a lost laptop or a compromised password)?

Typically this is discovered during routine audits. However, audits may be infrequent or recommendations from audits may be ignored. Therefore, for some organizations it takes an embarrassing event to bring attention to the issue. At its core, the biggest problem arises with the ever increasing use of personal devices in the workplace, such as mobile devices, or alternatively for those logging into work from their home computers or laptops.

The issue of BYOD ("Bring Your Own Device") to work has been on the radar of most large organizations for the last three to five years. Organizations are definitely trying to set policies around BYOD, but they are succeeding only to varying degrees. Presumably, the BYOD policy will stress that personal email accounts are never to be used for personal business. Unfortunately, in practicality this can be a challenge. When a device has multiple accounts attached to it, one can easily foresee the user erroneously sending a work-related email from a personal account. Once that happens, the recipients may reply to all, and the stage is set for a breach in the BYOD protocol.

What are some good tips for a company to prevent use of personal emails or applications for business purposes?

This goes to the core five sections of the BYOD policy, and the related procedures and guidelines. The key areas for a BYOD policy to cover include: 1) guidance on acceptable uses of personal devices to transact official business, including instructions on distinguishing personal email account usage from official business accounts; 2) a list of the types of sanctioned devices (e.g., Ipad, Blackberry, Iphone, etc.), and rules of engagement with IT; 3) logistics such as whether the company will reimburse for usage of the personal device; 4) a security section that addresses encryption and other features that must be enabled to protect the data in the event of a loss or breach; 5) a section on risks, liabilities and disclaimers to help protect the organization against the employee misuse of the device.

Armed with the BYOD policy, other organizational documents (e.g., Password, Cloud Computing or Social Networking policies) could get into the specifics of training and auditing the policy for compliance, as well as the frequency for these.

Who is at fault for user violation of email protocols?

Ultimately progress and the competition to stay on top of it are at fault. The adoption of technology has far outpaced the ability of organizations to keep up with them, including the State Department or any others in the government or private sector. Consumers and customers demand the immediacy facilitated by technology, so people, processes and procedures take a back seat in favor of adoption. In the ideal scenario, before any organization rolls out or permits any new technology (e.g., Blackberries, email tools, social media, content management, etc.), the

organization needs to vet its change management (i.e., a controlled roll-out that ensures proper user adoption and compliance), including its ability to audit and monitor compliance. In today's fast-paced world, however, the audit and monitoring part of the process is constantly a work in progress. Those looking for "fault" should be looking to fault those who do not learn from their experiences. In those instances, those in charge of the roll out of the program are at fault for not paying attention to system failures.

All that said, a corporate leader confronted with a systematic policy failure, coupled with high level (customer) demands to keep up with technology, faces a losing battle. The key is to strike a balance between controls and business needs. Few organizations have figured this out, so unfortunately for the State Department this could be a catalyst for more attention devoted to the change management and processes involved before the adoption of technology.

John Isaza is a California-based attorney, CEO of Information Governance Solutions, LLC and law Partner at RIMON, PC, a twenty-first century law firm that includes specialty in electronic information governance, records management and overall corporate compliance. He may be reached at John.Isaza@InfoGovSolutions.com or John.Isaza@RimonLaw.com. You can also follow him on Twitter and LinkedIn.