

# Peer to Peer

## Wireless Devices

mar

jun

sep

09

dec

Peer to Peer December 2009

## The Often Overlooked Mobile Security Gap

CATHY BRODE **3VIEW**

**W**hile the risks of inadvertent metadata disclosure are well understood within the legal industry, there is a security gap emerging via smartphones.

Despite the significant benefits of mobility, mobile devices introduce new security risks, especially if a firm's metadata removal application is limited to a desktop application. The mobile attorney using the Web or a mobile device does not have access to these tools and is at risk.

### MOBILE DEVICES ARE MAINSTREAM

The latest smartphone models are revolutionizing the way attorneys are working when away from the office. Every month, there are several business applications launched for smartphones specifically targeted at the legal sector. In addition to these, firms are increasingly developing their own mobile-enabled applications that hook into their enterprise applications such as practice management.

Although applications on mobile devices are highly unlikely to be exact replicas of those available on a desktop or laptop, they must still be included in risk assessments and your firm's security policy.

Security for such mobile devices needs to extend beyond just the physical security considerations, such as what happens if the device is stolen, encryption of communications and other standard security features like virus checking.

### THE MOBILE SECURITY GAP

While the risks of inadvertent metadata disclosure are

well understood by the legal industry, there is a security gap emerging via mobile devices that cannot be ignored. Although all business e-mail messages sent via a mobile device are routed through the firm's e-mail server and are covered by e-mail security functions at the gateway, it will bypass any desktop-based tools.

Users are now able to not only review documents via mobile devices, but they are also able to make minor edits to documents with more ease. But, as attorneys review and edit documents on their mobile devices and forward them to external recipients, the metadata in the document is fully retained and sent outside the firm. Even just forwarding an e-mail message with a document attachment from a mobile device bypasses any desktop metadata removal tool that is in place in the office.

Consider the following different scenarios:

- **Forward an e-mail message**

An assistant has just sent a document to an attorney who is about to board a plane. If the attorney has the capability, he might review it on a mobile device prior to forwarding it, and get the document on its way just before that plane door closes. Any document metadata resident within the originating document would then be exposed to the recipient.

- **Review, edit and forward**

With the availability of each new model of a smartphone, the power and screen size continue to increase. This leads to the greater ease by which documents might be reviewed on these models and, along with additional features, the greater the likelihood that attorneys will make minor edits to the documents

prior to forwarding them, either reattached to the original e-mail message or via a new e-mail message.

Taking that document sent to the attorney just before he boards the plane — he might decide to spend the flight reviewing the document and making any necessary amendments. After landing, he can hit the “send” button and off goes the document, metadata and all.

- **Attach a document to an e-mail message**

Mobile access to documents contained within a firm’s enterprise application such as a content management system (CMS) can allow an attorney to review or send a document via a mobile device. Such access might be either via a proprietary or in-house developed interface, and such systems typically come with access control mechanisms, but these might not provide metadata removal protection for mobile devices.

As with forwarding documents that have been received via e-mail, attaching a document to an e-mail message and sending it externally increases the risk of inadvertent leakage of information through the document metadata.

As the storage capacity of smartphones increases, so does the likelihood that documents will be downloaded and stored on these devices. At the very least, a policy should be in place to cover which business documents can be stored on a mobile device.

Metadata in the document will be retained in full for documents that are attached by the attorney to an e-mail message and sent externally. This applies both to documents that are stored on the smartphone and those that are stored within a central business system, such as a document management system (DMS) that is mobile enabled.

There are different metadata removal applications on the market today. Here is a list of features that should be considered when investing in this technology:

- **Wide service spectrum:** supports any e-mail client and e-mail server (BlackBerry, iPhone, PDA, netbooks and Webmail)
- **Multiple format support:** MS Office, PDF or OpenDocument Format
- **Automated system with low operational costs:** metadata is removed automatically according to centrally set rules. No user training or ongoing technical support is required, which substantially reduces the application lifecycle costs
- **Reduced risk of leakage:** no user intervention is required, which ensures a consistent service level and

reduces the risks of inadvertent data leakage

- **Application resides on network:** the automated system provides a service that is transparent to the user and works reliably, out of sight, on the company network. Removing metadata from documents is a processor intensive application for desktop or laptop computers, which can cause problems and severely degrade employee productivity. Transferring this processing to the network or via software as a service (SaaS) is especially important for organizations that send large quantities of documents via e-mail;
- **Ease of integration:** well documented application programming interfaces (API) enable ease of integration into DMS and CMS.

## THINK BEYOND THE OFFICE

So, not only do law firms need to have security policies in place for metadata scrubbing or removal from documents being forwarded by desktops within the office, but they also now need to look at how to protect themselves by scrubbing metadata from documents being forwarded outside the firm through a mobile device.

When looking at a solution, like one that scrubs document metadata as the document is sent via e-mail, ensure that it will cover not just desktops and laptops, but also any mobile device or mobile access method.

In addition, if your firm currently has a policy for use of just a single device, it is important, as with other applications, to bear in mind that this is likely to change. You should consider support for multiple types of mobile devices when evaluating solutions.

It is clear that smartphones and other mobile devices enable attorneys to conduct business efficiently. Ensuring that this is done securely does not mean limiting their capabilities to access, review, edit and send of documents. With the right security technology, features and considerations, your firm’s data can be secure whether on a desktop, laptop or mobile device. **ILTA**



Cathy Brode is Founder and Vice President of Product Marketing for 3BView ([www.3bview.com](http://www.3bview.com)). She has more than 20 years’ experience in the IT and life sciences industry. Prior to 3BView, Cathy was a founding member of CDC Solutions, a provider of software and services for the life sciences industry, which was acquired by Liquent in 2003. She was previously employed as a consultant at Kinesis Systems (now part of IBM) and, earlier in her career, managed a major European research project on advanced network management for Plessey Research. Cathy holds a degree in Computer Systems from University College Cardiff. She can be reached at [cathy.brode@3bview.com](mailto:cathy.brode@3bview.com).