InfoWorld

MODERNIZING ENTERPRISE IT

DIGITAL SPOTLIGHT FALL 2014 $29

Liquid Computing: The New Enterprise Workflow

Welcome to the liquid workflow

IF YOU'RE AROUND my age, your computing life began with a single screen. Today, you probably have three to five screens or more: a work computer, a smartphone, multiple home computers, maybe a tablet. Soon, you may add a smartwatch and a new wave of mini-devices ushered in by the Internet of things.

With this multiplicity, the idea that you have a "primary" device slips away. Instead, the heart of your compute experience rises to a cloud where you are at the center. For that ascent to be complete, however, each of your devices needs to be seamlessly connected with the others.

InfoWorld's executive editor, Galen Gruman, has coined a phrase for this: "liquid computing." As you'll see, Apple, Google, and Microsoft are already testing this new modality, so that your work—not just the data, but what you're doing with it at any given moment—can flow instantly to any device in your personal cloud ecosystem.

Liquid computing has far-reaching implications for business: The increase in productivity will be stunning, but the loss of control over data will cross an alarming threshold for many IT professionals.

In this Digital Spotlight, Galen, along with InfoWorld contributors Paul Roberts and Fahmida Rashid, examine the reactions of vendors and customers alike to this new reality. The redefinition of personal computing couldn't be more profound.

—Eric Knorr, *Editor in Chief*

INSIDE

Mobility marches on.

Mobility doesn't stand still. It moves in every direction but backward. No matter where you are on the mobility journey, you need to know about Citrix XenMobile, the only comprehensive, future-proof enterprise mobility management solution.

With enterprise-grade mobile device, mobile app and mobile content management, plus business productivity apps and secure email, you can address your most critical mobility needs now and seamlessly add capabilities as the business evolves.

Make the next move. Citrix XenMobile enterprise mobility management.

citrix.com/solutions/enterprise-mobility

CITRIX®

Welcome to the next tech revolution:

Liquid computing

Cloud computing has already changed the way we work. Soon, our own personal clouds will enable us to pick up where we left off seamlessly as we move from device to device. BY GALEN GRUMAN

IMAGINE YOU'RE IN the break room, typing an email on your tablet, when a colleague interrupts you. Later you return to your office and lay the tablet on your desk. An icon appears on the screen of your office laptop. You click it and up pops the partially completed email you were just composing on the tablet.

This advanced functionality already exists in the form of the Handoff feature built into the iOS 8 and OS X Yosemite updates. It signals a change in computing that Google and Microsoft are also pursuing, not just Apple. Handoff is the first big step into a future where the notion of a device will be radically transformed.

At first glance, what Apple is doing is blurring the lines between mobile and desktop devices. That's true, but it's only part of the

actual transformation underway. At InfoWorld, we've given this transformation a name: liquid computing.

The Handoff feature and liquid computing in general foretell a world in which work is decoupled from device, and data flows along with the activities and movements of the worker. In the era of liquid computing, the device no longer occupies the center of the computer universe, as it has since the dawn of the PC era thirty years ago.

Think back to that time, when people first started getting PCs at home, not just at work. Remember the effort we all spent in making sure we copied our files to a disk for use at home? We had to bring our data with us or else use a network connection to a file share. That barrier exists to this day. Sure, your e-mail and work files may live in the cloud and can be accessed from many different types of devices. But the assumption is still that you work on a single device at a time – creating and then updating a master record. Moving to a different device necessitates a number of discrete actions:

When you no longer have to worry about where a file is or where you left off on a task, you'll work very differently than you do today.

stopping work on one device, saving the master record, then switching to your new device, and recalling that master record.

This mentality is now on its way out.

The journey to liquid computing

To understand why, we need to roll back the clock a few years. With the introduction of Google Docs and Google Apps, Google showed us a different way of thinking about computing and workflow, putting the cloud at the center of the computing environment. With Google Docs (now called Drive), you created your documents on its servers and worked on them there, usually through a browser but also via native apps on iOS and Android. You didn't have to sync your data because it was accessible from pretty much any device. That change was also mirrored in features introduced to most major Web browsers in recent years that offered "browser syncing" and disaggregated the browser (and its stored data) from the device it was running on. Today Web browsers sync passwords, URLs, and so on, making users accustomed to the notion that it doesn't matter what device they have at hand—the context in which they were working will persist, at least for Web activities.

The record will show that Google's Web-based apps don't work that well at least compared to what can be done on a smartphone, tablet, or PC native app. Today, most of us still start with the device and use the cloud mostly as a convenient file share. But cloud storage services such as Box and Dropbox reimagined that file share in a user-friendly way, with similar broad device support. Apple's iCloud Documents took the same idea but tied it to specific apps, moving us away from the notion of a common file pool to a common activity pool: text documents or spreadsheets or photos. Apple's initial iCloud Documents approach was too tied to its apps, but in iOS 8 and OS X Yosemite, Apple is expanding its cloud beyond its own applications.

Apple Handoff is currently the boldest foray into liquid computing, but both Google and Microsoft have taken similar (albeit baby) steps in that direction. The forthcoming Android L will support Handoff-like interactions between Android devices and Chrome OS computers. Of the main platform vendors, Microsoft is the least advanced, though it talks the talk and has made moves similar to Apple and Google in its syncing across Windows 8 devices and its Google-like mix of native and cloud apps for cloud-stored Office documents.

The effect of liquid computing on business

When you no longer have to worry about where a file is or where you left off on a task, you'll work very differently than you do today.

People who've adopted an iCloud-centered workflow, a Google-Drive centered workflow, or an Office 365-centered workflow know what I mean: You don't think about where files are, because they're wherever you have an Internet connection. You think much less about passwords and bookmarks, thanks to Apple's and Google's ability to remember them across devices, which means it's easier to take care of your needs wherever and whenever.

That's the fundamental conceit of liquid computing: Your activities, not just your data, flow from device to device. You might think that's simply cloud computing in action. It is—but Handoff and other similar features show that you don't need the cloud to do this. Specifically: Handoff can operate as a kind of peer-to-peer network, using Bluetooth and Wi-Fi Direct for iOS devices and Macs to

In the era of liquid computing, the device no longer occupies the center of the computer universe, as it has since the dawn of the PC era thirty years ago.

"notice" each other's presence, then compare notes as to what the user is doing on all nearby devices for which that user is signed in. That's Handoff, and it's much more powerful than simply making the same data available everywhere.

Of course, the "wherever and whenever" nature of Handoff freaks out most IT shops. After all, most are still struggling to make peace with BYOD (bring your own device), which filled enterprise environments with consumer smartphones and tablets. The movement of enterprise workflows between devices, some of which aren't under full control of IT, using a standard image and fully audited, makes IT governance much harder.

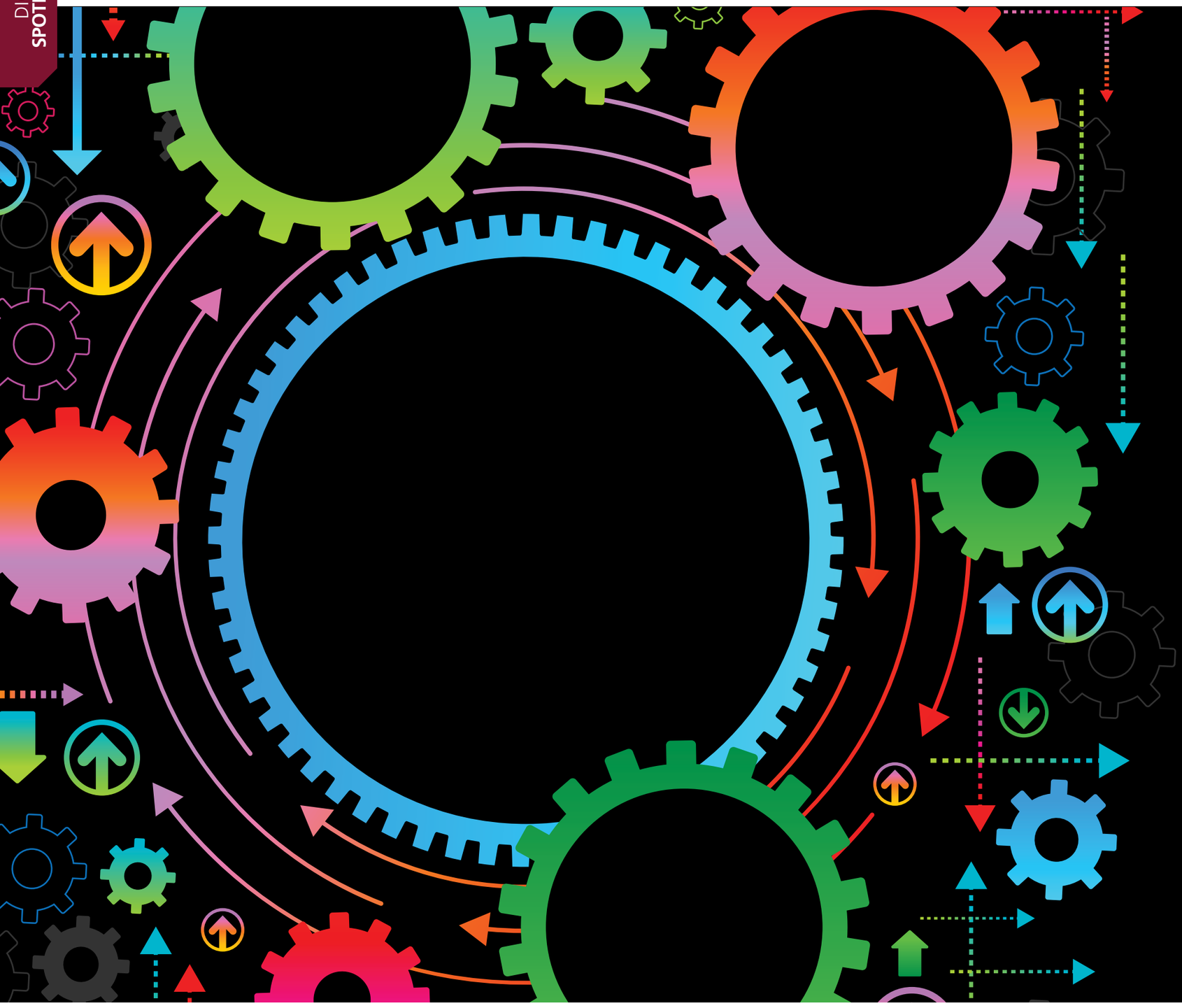
As it stands, features such as Handoff are resolutely consumer-focused. There is no way to audit such ad hoc workflows that traverse devices and don't need to go through a common network. Without auditing, you cannot assure compliance or security. There's already evidence that the underlying architecture of some next-generation connectivity features may be found wanting.

There are a few glimpses of how compliance and data management will work in a liquid computing world, but only glimpses. Users will again lead the way and introduce liquid computing even as their IT organizations rail against now-quaint notions like BYOD. IT and regulators will either figure it out or again get ignored or even be pushed out of the way. Ultimately, IT may have to let go of control (or the illusion of it) for the vast majority of data and workflows, using other means to validate access and information check-in/check-out and worrying less about what happens in between.

I truly believe that liquid computing will result in a major shift in how we work and think about computing devices. There'll be mistakes and failure along the way, but the basic notion simply makes too much sense. After all, it's how people naturally work: We "sync" and adapt through communications, even when under a hierarchical organization, using the tools we can find, not just those given to us.

When computing works more like us, watch out!

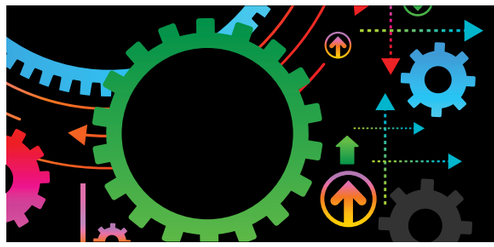
InfoWorld executive editor **Galen Gruman** *analyzes the latest issues in mobile technology and the Internet of things.*



Adapting enterprise workflows to mobile device continuity

Microsoft, Google, and Apple all envision a world in which data and workflow moves seamlessly between mobile devices in all shapes and sizes. That sounds cool. But are enterprises ready for the challenge?

BY PAUL ROBERTS



The shift to the cloud and mobile has the potential to make workers far more productive than ever before.

FOR MUCH OF the last thirty years, IT departments had a pretty clear goal: managing the interactions between back-end systems like application and database servers and a small range of client computers, mostly desktop systems and laptops.

The scope of that task was straightforward. Data resided in enterprise databases with a clear master record that could be recalled or modified by privileged users by way of an application running on a client system. Access to that data was restricted based on a user's role within the organization and the work he or she was tasked with. Access to the network on which the database, application server, and users all operated was further restricted using firewalls, user authentication schemes, intrusion detection sensors, and so on.

Sure, things often went sideways. But, in general, these controls ensured that enterprise workflows worked: Sensitive information didn't go wandering and information workers benefitted from technology while also acting in accordance with an organization's priorities and policies.

All that is changing — and fast. Over the past decade, cloud-based applications and SaaS have combined with a range of new, portable computing devices to alter both how we work and where we work. That revolution started with laptops and then smartphones. It is continuing as tablets and wearable technology such as smart watches and Google Glass become mainstream.

The multipeer model

The shift to the cloud and mobile has the potential to make workers far more productive than ever before. As we've noted, new features in the latest versions of Apple's mobile and desktop operating systems, iOS and OS X Yosemite (due out this fall) will introduce so-called "continuity" features like Apple Handoff that allow data and applications to switch fluidly between different end points belonging to the same user (that is, associated with the same Apple ID).

The use cases for those features, so far, are targeted at consumers. Apple's website promotes Handoff as an easy way to forward phone calls, text messages, and e-mail between different devices.

Connectivity features (broadly defined) are likely to become the foundation for far more diverse kinds of peer-to-peer networking between individuals. For ex-

Securing ephemeral peer-to-peer or mobile mesh networks just isn't on the radar.

ample, developer documentation for Handoff includes a feature called Continuation Streams that seems to support bidirectional data flows between devices connected using Handoff, not simply a mirroring of one application from a host device to a client. It's unclear, however, how that feature will work.

The next version of OS X Yosemite also will support iOS 7's Multipeer Connectivity feature (the technology behind proximity-based chat apps such as Firechat). That could be used to create mesh-style networks of iOS devices or facilitate file sharing within offices.

Apple isn't alone. Google executives have also talked up concepts like mesh networking and peer-to-peer connectivity in recent months. Google sees those capabilities as a way to tie together devices running its Android mobile operating system, including mobile phones, tablets, wearable devices, and home automation technology.

Eyes on the future

What will this brave new world look like? Nobody knows for sure. But if you want to assess what's to come as companies assess trends like mobility, wearable tech, and multi-peer-connected devices, examine forward-looking verticals such as healthcare and retail.

In these settings, workers are already embracing next-generation devices such as Google Glass, remote sensing, and proximity-based networking. Their experience points the way to what promises to be a bright, albeit complex, future of work.

To get a sense of what the future looks like, look to companies like CrowdOptic, a San Francisco-based start-up that makes technology that can use an individual's gaze to make context-specific associations and take specific actions. The company occupies a niche Gartner is calling "context-aware computing." It was one of just a handful of firms named by Google as a "Glass at Work Certified Partner."

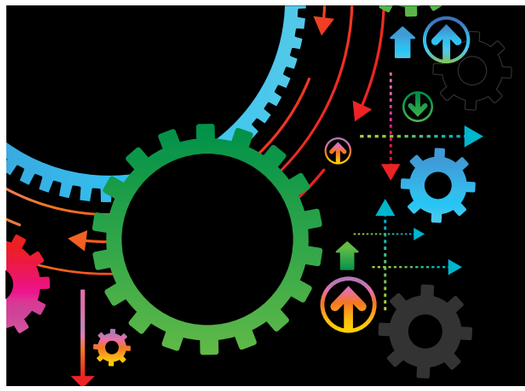
Jon Fisher, CrowdOptic's CEO and founder, said that the company's secret sauce is understanding, in real time, where the mobile devices on its platform are aimed. That new factor — focus or "gaze," if you like — enables a slew of what Fisher calls "black magic applications." They include allowing the devices to share points of view.

"From a workflow perspective, deploying smart glasses with this context is gold in sports, entertainment, medical, building, and — perhaps most of all — first responders and government, like police, fire, etc.," Fisher said in an e-mail exchange.

No surprise: Many of CrowdOptic's applications today are in advertising (place-sensitive and context-sensitive ads and displays for platforms like Glass), broadcasting (live sporting events from the player's perspective), and physical security (spotting disturbances or important events in large crowds).

Improving health

Promising applications proliferate in health care as well. In July, CrowdOptic



"Fortunately, there's little chance that rank-and-file enterprises will need to wrestle any time soon with questions about the best and most secure way to implement wearables." – PAUL DEPOND, vice president of technology and innovation at Globo PLC

announced that it is working with Stanford University School of Medicine's cardiothoracic surgery department to use its software to improve resident training in complex surgical procedures using Google Glass. Essentially, CrowdOptic's software will allow attending surgeons to "inherit" the point of view of the surgical resident simply by gazing at them. In the process, they will see what the intern is seeing.

That has huge implications for teaching delicate surgical procedures in the confines of an operating room, where attending surgeons have difficulty sharing the exact field of view as their trainees.

Another medical application highlighted by Google concerns the use of Glass by primary care physicians during patient interviews and screening. The trial, by Google and the firm Augmedix, outfitted physicians with Google Glass running Augmedix's software. The software captured the information from doctor-patient visits and streamed it to back-end systems where artificial intelligence software (and human operators) used the data to update the patient's chart in real time. Physicians can also use voice commands to call up data from the patient's chart, which appears on Glass before their eyes.

The technology has been a productivity boon. Physicians at the Ventura, California, clinic where the trial took place reported a decrease in the total daily time spent entering data into electronic health record systems from 33 percent to 9 percent and an increase in direct patient care from 35 percent to 70 percent.

The promise and the peril

Although these are only trials, they suggest ways in which other workflows, piped through wearable devices like Glass, could become fused with the bodies and physical context of users. To transfer a file to a coworker, just look at the person and say, "send file." To email, simply start speaking, and so on.

But they also suggests some of the possible pitfalls. For the Google and Augmedix trial, the Google Glass devices worn by physicians were locked down to only run Augmedix's software and only on the clinic's secure and encrypted network. No Internet access from the Glass device was allowed, nor were other applications.

Fortunately, there's little chance that rank-and-file enterprises will need to wrestle any time soon with questions about the best and most secure way to implement wearables, says Paul DePond, vice president of

For now, most organizations need to crawl before they can walk, let alone fly.

technology and innovation at Globo PLC. Globo makes enterprise mobility management technology for customers across industries, including healthcare.

The facts on the ground in almost every industry are that companies are still struggling to reign in smartphones using basic mobile device management features, DePond said. Securing ephemeral peer-to-peer or mobile mesh networks just isn't on the radar.

Most of Globo's customers are focused on managing the security of employee-owned mobile devices and possibly leveraging custom mobile applications for important functions that are still confined to the desktop, or even paper, he said.

Still, DePond thinks many of the same technical hurdles that companies face around managing mobile devices and applications will transfer to devices with "mesh networking" features and next-generation platforms like Google Glass

"The best way we saw to solve the BYOD problem was to create a secure workspace on the device. That workspace is the only element that company says 'this is ours.' The rest, you can do what you want with."

Using secure and encrypted virtual containers to house company data and applications allows Globo and its customers to enforce granular controls that might not be native to the platform or the OS. For example, Globo customers on smartphones can use a secure chat feature to communicate. But that app doesn't allow them to copy or paste content from the chats to other applications, or even to take screenshots of the application.

The same secure container concept may also work well on wearable platforms, DePond said. However, before that can even happen, third-party providers like Globo need tools: APIs that they can hook into, clear documentation of features, and ideally, standards that they can develop to that will be reliable across platforms. "Someone has to put an API out there to do stuff like that — turn features on and off, wipe data, and so on," he said.

For now, most organizations need to crawl before they can walk, let alone fly. That means bringing mobile devices under the same kind of control that exists for PCs: managing software updates and patches, segregating sensitive functions from consumer functions, and picking low-hanging fruit with commercial or custom mobile apps suited to niche purposes within the organization.

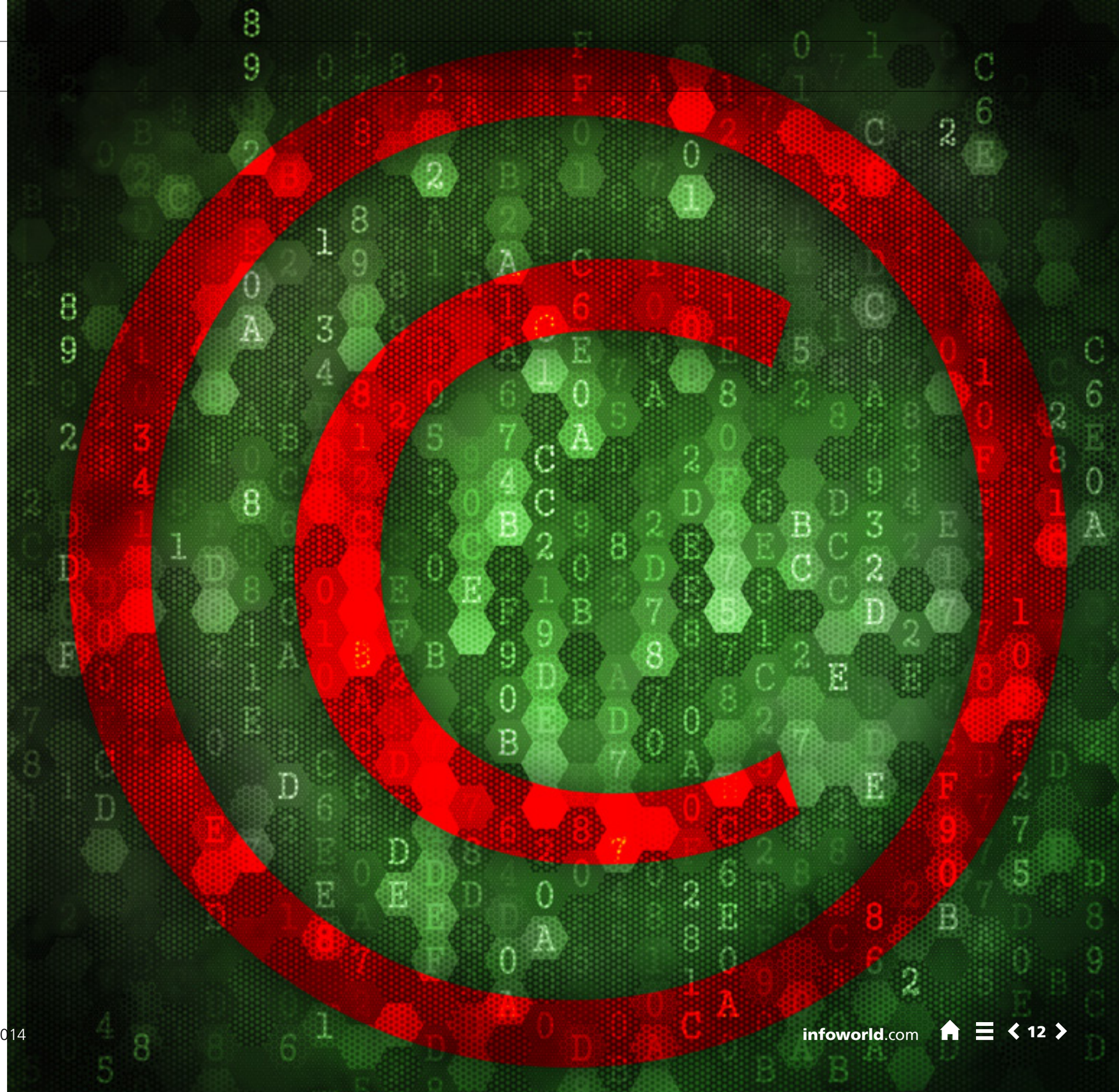
Assuming they can get all that to work, companies may be ready to ascend to the truly awe-inspiring heights that these new technologies suggest.

Paul Roberts *is a former senior editor for InfoWorld who writes about hacking, cyber threats, and information technology security. He edits The Security Ledger, a blog focused on securing the Internet of things.*

Is it time for DRM's second act?

Powerful new peer-to-peer connectivity features in products being developed by Apple, Google, and Microsoft will add security risk. One solution: content-based protections such as digital rights management.

BY PAUL ROBERTS



IF YOU'RE AN information security professional working in an enterprise setting, the last decade hasn't been kind. Malicious software has become more powerful and stealthy. Traditional security and detection tools such as antivirus and intrusion detection have struggled, unsuccessfully, to keep pace.

During the same period, the advent of smart, powerful mobile devices like iOS and Android phones and tablets have knocked down what few bricks remained in the hardened enterprise perimeter. Consumer-driven BYOD (bring your own device) is now the *de facto* (if not *de jure*) policy in most workplaces. Still, mobile device management suites have only recently begun to gain wide adoption.

Now the tables are turning again. New, "liquid" workflows and the introduction of peer-to-peer connectivity features in mobile and end point operating systems by Apple, Google, and Microsoft promise to enable mobile devices of all types to work collaboratively and fluidly: sharing work and passing off data seamlessly.

But those same features threaten to break existing IT security and management controls. As documents and data begin to move fluidly between devices controlled by a single employee or a team of them, enterprise IT shops may be forced to reconfigure (or just relax) existing process controls such as user authentication, configuration management, and access control. What will take their place?

For your eyes only

One possible scenario, say IT security and mobility experts, is that the shift to "liquid" workflows and peer-to-peer connectivity may herald renewed enterprise interest in so-called DRM (digital rights management) technologies that place granular content- and context-sensitive controls on the data itself. In fact, DRM's second act many already be well underway.

Scott Walker, who works in information security at DuPont, says that a number of efforts are in place at his company to better manage security policies across an IT landscape that is increasingly populated by smartphones, tablets, and other mobile end points.

"We really see mobile device use as inevitable," Walker says. DuPont workers—especially newer workers from the millennial generation—are clamoring to use tablets and mobile phones. That's pulling DuPont's IT department along. "We have an open culture," Walker says. "We want to enable people to do their jobs."

Apple's Handoff and similar connectivity features are not on the short list of features his company is looking at. However, DuPont does strive to create a "consumer-like" experience for workers, whether that means social network-like sharing and communications features for the corporate intranet or support for mobile devices and cloud-based document sharing at work.

But keep in mind, DuPont is the world's third largest chemical company. It has developed a roster of specialized materials that have become household names: nylon, Teflon, Mylar, Kevlar and Lycra. The company holds patents for technologies

Consumer-driven BYOD (bring your own device) is now the *de facto* (if not *de jure*) policy in most workplaces.

and processes worth billions of dollars, and its ongoing research is the object of intense interest to competitors at home and abroad.

For those reasons, Walker says the company makes data security the top priority. On its network and traditional end points, DuPont relies on a full contingent of enterprise protection tools: anti-malware, network- and host intrusion prevention. Data leak protection software from Digital Guardian blocks sensitive information from leaving the company's network.

DuPont currently uses a mobile device management platform to allow employees to send and receive corporate email from their smartphones. It has a limited deployment of DRM technology from RSA (now part of EMC). But the company's experience with that technology makes Walker wary: The difficulty of using the system meant it was extended to a small fraction of DuPont's documents and employees. "I look at that experience and feel like we really need to learn our lesson," Walker says.

Securing the cloud

Today, DuPont is investing heavily in SharePoint and Microsoft's Rights Management Services to secure and manage access to sensitive documents for employees and third-party contractors and supply-chain partners.

DuPont moves carefully around initiatives such as mobile and cloud adoption, wary of losing control of sensitive documents and data. Walker says the attractiveness of collaborative and productivity features such as Handoff and Apple Connectivity would be contingent on reassurances that the security of the data at rest and in motion wasn't being compromised in the process.

"If I'm going to put my sensitive data in your cloud, you have to assure me that you're going to protect it as well as I do," he says.

Apple's iCloud is the linchpin of its Handoff and Continuity services. Devices that use the Handoff feature need to be logged into Apple's iCloud with the same Apple ID. Developers will use Apple-provided APIs to invoke Handoff and desig-

"Data protection is the greatest concern organizations have with respect to mobility. Organizations manage the device and applications as a means toward protecting the data."

– **ROB SMITH**, analyst at Gartner

nate specific activities as shareable between devices ("open document," "read document," "edit document"). iCloud facilitates the pairing between WiFi-enabled and Bluetooth-enabled end points. The initial transaction may be peer-to-peer, but real data synchronization is handled through iCloud, according to Apple's documentation.

Apple does not provide much information about the security of iCloud or of the communications that make up Handoff exchanges. There is reason to believe that the technology may not stand up to the kind of scrutiny enterprise IT departments require. At the recent Black Hat Briefings in Las Vegas, security researcher Alban Diquet demonstrated security flaws in Apple's multipeer Connectivity platform that could allow a knowledgeable hacker to conduct man-in-the-middle attacks that stripped encryption protections from communications between two Apple devices.

Even if Handoff proves its mettle, Apple is not likely to cede to enterprises the kind of control they would want to feel comfortable storing sensitive information in iCloud. That may mean Apple Handoff—if not handoff-like features—has limited appeal.

"Fundamentally, the question for enterprises and Apple Handoff is 'Do you trust iCloud?' " says Rob Smith, an analyst at Gartner. "If the answer to that is no, then this feature will never work for you."

Which isn't to say that enterprises won't trust any third-party clouds. Smith says Microsoft has helped break down the IT department's resistance to the notion of integrated on-premises and cloud infrastructure with its Office 365.

"Enterprises are open to cloud, but with a level of control," Smith says. "Customers need to be able to institute some kind of control, but they don't care as much where it's hosted."

DRM to the rescue... eventually

DRM features—reimagined—may be that bridge. Walker says DuPont would love to have a mobile management platform that allowed it to enforce some kind of security policies and restraints on mobile devices and the data moving to and from them, especially given DuPont's close cooperation with its many supply-chain partners.

"You'd like to be able to track when and how many times the document was touched or opened," he says. "That kind of technology would give you some degree of control after the document left the premises." But the company hasn't

seen that kind of offering yet.

Salo Fajer, CTO at data protection firm Digital Guardian, says one of the top issues he hears from chief security officers is how to protect data as it moves between cloud and end point. "Companies want to be able to control and audit those movements and enforce policies around them. Who can open what and where." That's true no matter if the data in question is stored locally, on a network file share, in the cloud, or on an iPad, he says.

Existing technologies do a good job of protecting and monitoring data in transit: wrapping access policies around objects like email messages or documents and providing access control as well as an audit trail. Those capabilities are starting to reach to the cloud, extending access controls to hosted environments and mobile end points, Fajer says.

The kind of seamless movement that Apple is introducing with Handoff will be a challenge, Fajer admits. The key will be whether Apple (or Google or Microsoft) creates APIs that give application developers the ability to wrap security and policy around the data that is shared between devices using Handoff, Connectivity, and other features.

"If I'm going to put my sensitive data in your cloud, you have to assure me that you're going to protect it as well as I do."

– **SCOTT WALKER,** information security at DuPont

Hybrid solutions for today

For now, Gartner recommends that enterprises consider hybrid solutions that combine elements of end point protection and what it calls end point mobility management (EMM) technology, which comprises policy and configuration management for mobile platforms.

Some vendors are already moving beyond that, introducing "mobile content management" technology that can transparently encrypt files as they leave a PC or mobile device. Sophos, the antivirus software vendor, is one example of a company that's transitioning from end point-based protection to content-based protection, Gartner's Smith says.

In the months ahead, larger EMM vendors, including IBM, Citrix, and Good Technologies are likely to follow suit, as the focus of protection pivots from end point devices (laptops, mobile devices) to the data that moves between them. "Data protection is the greatest concern organizations have with respect to mobility," Gartner noted in a recent report on the EMM space. "Organizations manage the device and applications as a means toward protecting the data."

Where does that leave corporations like DuPont that are concerned with security and privacy? On the sidelines, at least for now, says Walker.

"We're a company that's going to go with what's known and sure. We're not going to be on the cutting edge of sharing and connectivity, and that's OK," he says. At some point, he expects that features such as Handoff will mature to a point that companies like DuPont can use them. But moving before all the requirements are met doesn't strike Walker as prudent. "You've gotta bring the goods security-wise," he says.

Paul Roberts *is a former senior editor for InfoWorld who writes about hacking, cyber threats, and information technology security. He edits The Security Ledger, a blog focused on securing the Internet of things.*

Connectivity vs. compliance: Can they get along?

The industry is readying new, multipeer connectivity features. They'll be a boon for worker productivity. But will they also break your compliance policies?

BY FAHMIDA Y. RASHID

Technology giants such as Apple, Google, and Microsoft are quietly experimenting with new networking and connectivity features that could bring explosive changes to the way users interact with and exchange information on enterprise networks. But for companies contemplating so-called liquid computing technologies such as multipeer connectivity and mesh networking, the question is whether the features might undermine hard-won compliance and security goals.

With liquid computing features like Apple's Handoff still in their infancy, enterprises are left guessing about how well prepared they will

be for this new age of decentralized networking. But the experts we consulted said the challenges these technologies introduce are not so different from what organizations are facing today with the advent of powerful mobile devices. It turns out that organizations with a good grasp of BYOD policies and security are well poised to face the regulatory challenge that will come with liquid computing features like multipeer connectivity and mesh networking.

As a phrase, "liquid computing" works on many different levels, says Paul Luehr, the chief privacy officer and managing director of Stroz Friedberg, an intelligence, investigations, and risk services firm. The image of liquid computing describes the fluid movement of data between connected, mobile endpoints, he said, but it also "appropriately captures the notion that data continuously wants to spill over networks and devices without resistance."

The notion of data that will flow seamlessly across devices holds the promise of enormous productivity gains. Imagine a health care facility where doctors and nurses can use features like Apple's (coming) Handoff to continue to manage a patient's treatment as they move between the hospital, clinic, and their homes, as one example. The productivity and efficiency gains alone make the concept of "liquid computing" encapsulated by Handoff intriguing.

The compliance hurdle

But the same scenario makes compliance-focused IT teams blanch. Personally identifiable patient information bouncing back and forth between secure and insecure systems? It may be tempting to simply block the technology over compliance concerns.

However, security experts we consulted expect that liquid computing wouldn't be such a big adjustment, after all. From a compliance officer's perspective, liquid computing's constituent elements like multipeer connectivity and mesh networking raise many of the same issues already addressed by the BYOD revolution that brought smartphones and tablets to the office. Both require organizations to track who is accessing what information, says Vijay Basani, co-founder and CEO of EiQ Networks, a company specializing in compliance and risk solutions. Regulations focus on "who is accessing what data and from which device," Basani says. The actual mechanics for tracking that information has always been up to the individual organization.

That said, assessing how liquid computing matches up against existing regulations is difficult. Compliance rules and regulations are industry-specific in the United States, Luehr said. While some mandates are considered prescriptive—such as the Payment Card Industry-Data Security Standard (PCI-DSS)—most are not, leaving the interpretation up to individual organizations. This means it's easier to be rigid and assume anything new would be forbidden, even if that isn't the case.

"Anytime you are talking about new technology and regulations and compliance, policymakers and regulators naturally are going to find themselves behind the curve," Luehr says.

In contrast, Europe and other regions treat data secu-

rity and privacy holistically, making it easier to bend them to apply to new technology innovations for which adoption might stretch across vertical industries.

Evolution, not revolution

Liquid computing is a continuation of modern computing trends that resulted in the Internet and wireless networking, notes Luehr. Organizations that have figured out how to manage these blended technologies and the expanded perimeter each entails are better suited to take advantage of the next wave, in which peer-to-peer connectivity will dissolve that perimeter entirely.

For example, the importance of knowing where the data is being stored, how the data is protected, who has access to it, and what happens when something goes wrong will remain the same whether the discussion is about BYOD or liquid computing, says Cliff Baker, founder and managing partner of Meditology, a health care consulting group.

Data is already distributed across multiple systems and networks in the health care world, and the Health Insurance Portability and Accountability Act (HIPAA) defines rules for data security, privacy, and breach notification. Already, organizations have to ask providers about encrypted storage, verify all data transfers are encrypted, and define access controls to restrict who can view the data.

Under HIPAA, the organization bears the ultimate responsibility for making sure the data is secure, regardless of its location, Baker says. Practically, this may very well mean that Apple's iCloud will be out of the question for hospitals. But it doesn't mean that plenty of other third-party providers will keep secure storage in mind as they build out liquid capabilities, he predicts.

Regardless of the technology's workings, authentication and validation will have to be integrated in how data moves across locations, Basani says. There will have to be some kind of a handoff to verify the destination device, if only to make sure a user's files don't flow onto an unauthorized (or rogue) device. User verification will be necessary to ensure the user owns both devices or the recipient is authorized to receive data.

Whatever authentication system is in place, whether it's through Apple's iCloud, Google's credentials, or some other third-party system, that information can be logged, Basani says.

Regulations meet reality

As it stands, existing regulations can handle traditional document flows imagined by features like Apple Handoff. But new forms of communications—like broadly adopted multipeer mesh networks – could spur new regulatory rules, Luehr says. For example, if electronic health records can flow across devices and be modified, new definitions would be necessary.

Organizations are already struggling with the fact that text messaging and other new out-of-network communications are not being captured, but they are still expected to provide that information as part of litigation proceedings. Liquid computing will increase the amount and types of data

currently not being collected, forcing regulators to make some changes, Luehr predicts.

One by-product may be that increased data flow leads to potentially new types of man-in-the-middle attacks and data breaches, Luehr says. At the recent Black Hat Briefings, for example, security researcher Alban Diquet demonstrated a method for conducting man-in-the-middle attacks against Apple's Multipeer Connectivity feature, which was first introduced in iOS 7. Diquet was able to show how a knowledgeable attacker could take advantage of weaknesses in Apple's implementation of the feature to force two clients into exchanging data in the clear (that is, without requiring encryption or authentication).

Developments like that in the threat landscape may mean that regulators will have to reconsider breach notification rules. Breach notification laws will have to redefine what constitutes a breach and figure out appropriate levels of communication.

The privacy conundrum

Another area regulators will have to pay attention to: consumer privacy. Users are increasingly worried about how situational metadata, such as what device they are using, their geographic location, and what applications they run, can be used by advertisers or the government to understand (and monitor) their behavior. Already, website owners and app developers have to tread carefully when collecting data about their customers and visitors to online properties.

Regulatory agencies and privacy officials are increasingly aware that global identifiers can be tied back to an individual other than first and last names, and users are just as sensitive to having that information exposed, either in a data breach or to advertisers.

One example: The Federal Trade Commission has begun to broaden its definition of personally identifiable information from more than the name, address, and account number to include device number and location.

Features like Apple Handoff and mesh networking could amplify personal privacy concerns by growing this pool of identifying information with insights such as what time of the day the individual uses certain devices, what kind of computing is done on which device, what tools and services the person uses, and how many devices the individual has, to name a few. The elevation of consumer identities (like Apple ID or Google account) to de-facto universal IDs may force regulators to redefine personally identifiable information to encompass these identifiers, Luehr suggests.

The unified data security theory

Eventually, organizations that haven't already done so will have to adopt a holistic approach to data security and shift away from the notion that data is either at rest or in motion, Luehr says. Legacy compliance systems tend to focus on where the data is stored or how it is being transferred. Liquid computing challenges the notion that you are in one state of another. Securing the device is still important, "but it may not actually protect the data because it may have already

Considering that compliance mandates don't change too frequently and tend to be additive, it's a fact that technology will always outpace laws and regulations.

drifted over to another device," Luehr says. "Sometimes it's not just about what you say, but also where you are."

Considering that compliance mandates don't change too frequently and tend to be additive, it's a fact that technology will always outpace laws and regulations. This poses challenges for both policymakers, who have to figure out ways to keep the requirements relevant, and implementers, who want to take advantage of the technology but may find their hands tied because the regulations are outdated.

"Liquid computing may be here tomorrow, but it will be a couple years before regulations even come into play," Basani says. "BYOD took several years before it became standard."

In the final analysis, the types of advances that comprise what we're calling "liquid computing" underscore a key tenet to security: Security is not a destination, but a process.

Fahmida Y. Rashid *is a veteran business and technology journalist living in the greater New York City area.*

InfoWorld
MODERNIZING ENTERPRISE IT

www.infoworld.com

InfoWorld
501 Second St.
San Francisco, CA 94107
415.978.3200

EDITORIAL

Editor in Chief
Eric Knorr

Executive Editor
Galen Gruman

Executive Editor, Reviews
Doug Dineley

Managing Editor
Uyen Phan

Senior Editor
Jason Snyder

Editor at Large
Paul Krill

Senior Writer
Serdar Yegulalp

East Coast Site Editor
Caroline Craig

Newsletter Editor
Lisa Schmeiser

Associate Editor
Pete Babb

Senior Online Production Editor
Lisa Blackwelder

SALES

Senior Vice President Digital / Publisher
Sean Weglage
508-820-8246

Vice President, Digital Sales
Farrah Forbes
508-202-4468

Account Coordinator
Christina Donahue
508-620-7760

East, Southeast, IL and MI
Chip Zaboroski
508-820-8279

East, New England, New York
Chris Rogers
603.583.5044

West / Central
Becky Bogart
949.713.5153

N. CA / OR / WA
Kristi Nelson
415.978.3313

Images by Thinkstock

IDG Enterprise
An IDG Communications Company

IDG Enterprise
492 Old Connecticut Path, P.O. Box 9208
Framingham, MA 01701-9208
508.879.0700 (Fax) 508.875.4394

CEO
Matthew Yorke
508-766-5656

Executive Assistant to the CEO
Nelva Riley
508-820-8105

SALES

Senior Vice President, Digital Sales
Brian Glynn
508.935.4586

Senior Vice President Digital / Publisher
Sean Weglage
508-820-8246

CIRCULATION

Circulation Manager
Diana Turco
508.820.8167

CUSTOM SOLUTIONS GROUP

Senior Vice President
Charles Lee
508.935.4796

DIGITAL SOLUTIONS GROUP

Senior Vice President / General Manager
Gregg Pinsky
508.271.8013

EDITORIAL

Senior Vice President / Chief Content Officer
John Gallant
508.766.5426

EVENTS

Senior Vice President
Ellen Daly
508.935.4273

FINANCE & OPERATIONS

Senior Vice President / COO
Matthew C. Smith
508.935.4038

HUMAN RESOURCES

Senior Vice President
Patty Chisholm
508.935.4734

IDG LIST RENTAL SERVICES

Director of List Management
Steve Tozeski
Toll free 800.IDG.LIST (U.S. only)
Direct 508.370.0822

MARKETING

Vice President
Sue Yanovitch
508.935.4448

Resources

SPONSORED BY: CITRIX®

White Paper:
Drive Business Growth with Mobile Workspaces

Discover how you can empower people to get their work done in an always-on, fully secure environment that follows workers anywhere, on any device or network.

DOWNLOAD HERE

Infographic:
Mobile Workspaces: Enable People with New Ways to Work

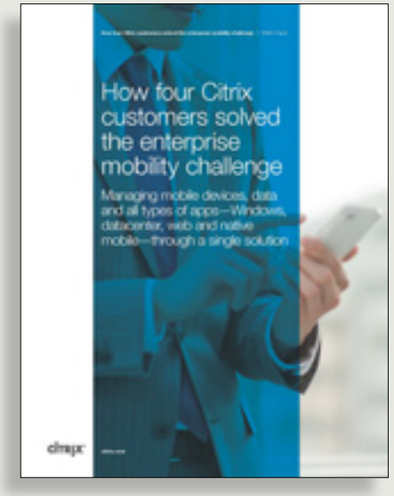
Find out why the mobile workspace is the way to work better.

DOWNLOAD HERE

Gartner Report:
Best Practices in Choosing, Implementing and Using MDM and EMM

Take a look at best practices for evaluating and selecting an EMM solution in this Gartner report.

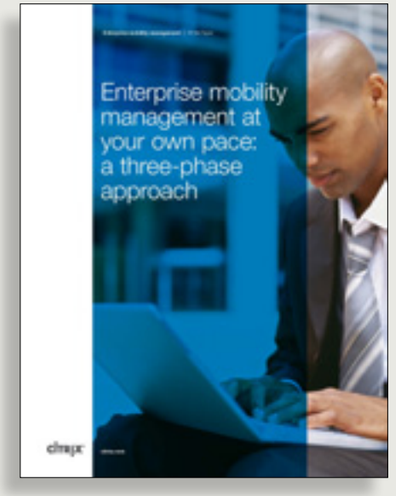
DOWNLOAD HERE



White Paper:
How Four Citrix Customers Solved the Enterprise Mobility Challenge

Manage mobile devices, data and all types of apps—Windows, datacenter, web and native mobile—through a single solution.

DOWNLOAD HERE



White Paper:
Enterprise Mobility Management at Your Own Pace: A Three-Phase Approach

Learn about a three-phase plan for mobile empowerment, management and security using the Citrix XenMobile EMM platform.

DOWNLOAD HERE