# Mobile content

## has made Anders Andersson a lucky man.

An avid fan of the 2004 Summer Olympic Games in Athens, he was worried that his day job and long hours would prevent him from watching track and field events and following his favorite Swedish athlete Carolina Klüft, who competes in the heptathlon and long jump events.

But TeliaSonera, the leading telecommunications provider in the Nordic-Baltic region, has come up with solution that will allow Andersson to keep up with coverage even on the bus to work. It has rolled out Sweden s first large-scale mobile television broadcast service, allowing Andersson and thousands like him to watch the Olympics anywhere, anytime on a 3G-enabled handset for free.



## Protecting Mobile Content

**PEGGY ANNE SALZ**

In neighboring Finland, TeliaSonera has launched a service designed to change the way users listen to—and interact with—music. In June, it became the first operator in Europe to "air" Sony's StreamMan. The mobile service allows users with Nokia 6600 and Ericsson P800 and P900 smartphones to listen to music, create playlists, and share their experience with friends.

TeliaSonera is one of a growing number of mobile access providers making the transformation from network operator to broadcast operator. Eden Zoller, a research director at Ovum in the U.K., keeps a sharp eye on this shift. "People don't like missing their favorite TV shows and will use mobile to catch up," she says. Moreover, the perfect fit between mobile and music—as demonstrated by the growing popularity of portable playback devices—gives service providers good reason to fine-tune their mobile music offerings to include video clips, music downloads, and artist updates.

But there's a catch. Previously, mobile content—ringtones, screen savers, and logos—was mass market and low value. So a primitive forward-lock feature on mobile phones that prevented most mobile users from passing content among peers was deemed satisfactory, and many top-name content owners went along with the scheme. Today, the distribution of rich multimedia content such as music downloads and video clips mandates a much more stringent approach to digital rights management (DRM).

"DRM is essential to create a sustainable multimedia content offering online and on the mobile," observes Paul Jackson, a senior analyst with Forrester Research in Amsterdam. If operators want to deliver premium content, he argues, they will need to satisfy content owners' requirements to control and charge for that content. At the same time, DRM will have to bend to users' demands for a content service that allows them to have the freedom to use their content as they like. That includes the ability to access it, port it, and distribute it across a number of devices and platforms.

And that's where the DRM dilemma begins.

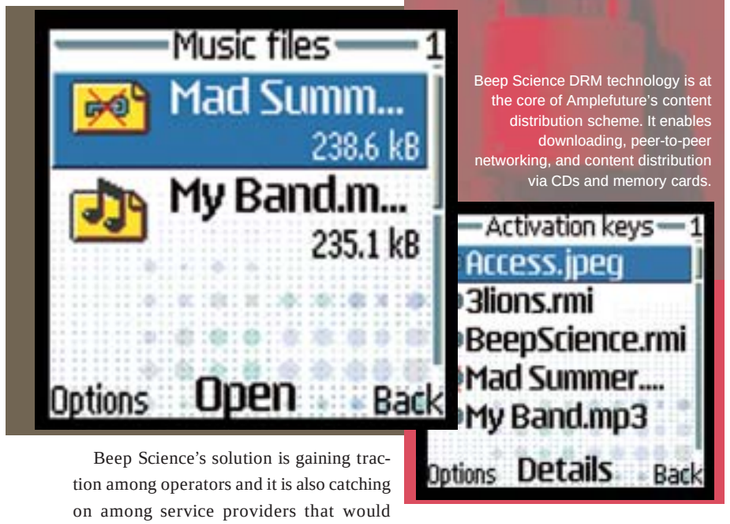
### PLAY IT AGAIN (AND AGAIN)

"Usability is critical to gaining acceptance (for DRM solutions) from end users," notes Markku Mehtala, VP of business development at Beep Science, a Norway-based provider of client- and server-side DRM software solutions. Content protection must be flexible enough to allow users to play purchased content on multiple devices and move purchased content when they change devices.

"The challenge going ahead is to deliver a seamless customer experience—and still enable the content owners and rights holders to remain in control of their digital assets," Mehtala says. The convergence of PDAs, mobile phones, and portable playback devices "creates the necessity for DRM solutions that encourage anytime, anywhere, and any-device access to content, but draw the line at piracy."

To this end, Beep Science has developed a product portfolio of standards-compliant DRM solutions that can protect and manage rich multimedia content in distribution. The technology effectively hides "fingerprints"—or telltale lines of software code—within the content delivered to the user's device. This method of content encryption also enables secure super-distribution. "When the user sends the content from his device, the recipient of the content receives it but can't access it without acquiring usage rights from the service provider—and so the Beep Science DRM solution—first," Mehtala explains.

Moreover, the DRM technology allows users to share content offline between several devices, download content from a PC using broadband to a portable device, or transfer files from an old device to a new one without having to download new licenses or content objects.




Beep Science DRM technology is at the core of Amplefuture's content distribution scheme. It enables downloading, peer-to-peer networking, and content distribution via CDs and memory cards.

Beep Science's solution is gaining traction among operators and it is also catching on among service providers that would rather roll out their own DRM services than wait for operators to pick up the pace. "By providing our clients secure end-to-end digital content distribution across mobile networks with fair rewards, we ensure that paid content has a future in mobile," says Rob Ellis of Amplefuture, a U.K.-based distributor and aggregator of mobile content whose client list includes 65% of the country's ISPs, as well as media companies and music labels.

Ellis says that its DRM capability will allow his company access to a wider range of content such as mobile games, ringtones, realtones, wallpapers, and screensavers, and to attract many more top-notch media brands. "The lack of credible DRM systems has been a barrier to many content owners such as TV production companies, animators, music companies, and individual artists to getting involved in the mobile space," he explains. "Our DRM capability gives them the confidence they need to enter the market on a commercial scale."

## THE STAKES

Developments like this could make the next six to twelve months the most interesting, according to Trevor Brignall, a business development director at Capgemini's Telecom, Media & Entertainment division. "We're likely to see DRM equipment that is technology independent and neutral," he says. The market will also see the appearance of long-awaited DRM solutions that cover the content value chain from licensing content to billing the customer.

Consider a service provider that cleverly combines previously unrelated images and music to create a new service. Brignall explains, "That provider will need a system that recognizes the difference between the two pieces of content and makes payments to different rights organizations." Moreover, he warns, providers will also need to be careful that they don't accidentally sell or market content in geographies where they don't have the rights to do so. It's a tall order given the nature of mobile and the tendency of users to roam networks.

Against this backdrop, DRM costs are likely to be considerable—but so is the payoff. Brignall estimates expenditures of "€5 per customer per month over time." Depending on factors such as user age and disposable income, the figure of €5 could "easily increase to €10 to €15 as services we don't know today are brought to market," says Brignall.

Ovum in the U.K. forecasts that worldwide revenues from wireless content services will increase fourfold: from a total of $9.1 billion in 2003 to $39.7 billion in 2007. "Achieving these revenues is dependent upon a DRM solution being in place," Ovum stresses. "In order to protect these revenues and ensure continuing growth beyond the forecast period, operators must have gained the trust of the content owners with regard to DRM and must have met the needs of the end users in one to three years."

The development of DRM in each region will also depend on the demand for wireless content services in the first place. Ovum estimates that, by 2007, approximately 37% of content revenues will be derived from Western Europe. Drivers are likely to include MMS and music download services. In contrast, North America is in an embryonic phase and currently accounts for just over 8% of global mobile content revenues. By 2007, North America should account for 21% of wireless content revenues. The Asia-Pacific market is a mix, with Japan and South Korea leading the way. The region will account for 28% of wireless content revenues; China and India will account for 7%.

## COME TOGETHER

Before the telecoms' downturn, analysts estimated that between 50 and 70 companies were developing or providing a DRM solution. This created confusion in the industry around DRM standards and widespread disagreement about the number of DRM solutions the market can support.

"Users want a seamless experience regardless of how many DRM schemes are out there," argues Forrester's Jackson. He believes a multitude of DRM standards can coexist as long as they remain invisible to the consumer. "It doesn't matter if some of them are proprietary. But, if users hit a wall of DRM incompatibility and can't move content from one device to another as they wish, then they're likely to turn away from the content altogether."

Sensing that this diversity could stunt the growth of the fledgling mobile content service industry, major players have thrown their weight behind standards. Leading the pack is the Open Mobile Alliance (OMA), an organization that was formed by the merger of the Open Mobile Architecture Initiative and the WAP Forum in 2002. So far, the OMA has brought together over 300 mobile operators, technology companies, and handset manufacturers to uphold and develop standards for wireless communications.

A milestone on the road to one DRM standard was this year's release of version 2.0 of the standard for mobile devices, known as OMA DRM 2.0. OMA DRM 2.0 is backward compatible with OMA DRM 1.0, a DRM standard designed with simple 2G mobile phones and low-cost content such as wallpaper and ringtones in mind. In contrast, OMA DRM 2.0 is designed for much more powerful feature-packed mobile devices that also have the ability to play and store high-resolution audio and video. But OMA DRM 2.0 may be too late. Indeed, devices are slated to appear on the market for the 2004 year-end holiday season but most deployments of that standard will only start in 2005.

"I think the big question each operator has to ask is: Do I want to make money now, or in the future?" notes Guilio Panzera, customer product manager for Music2You (M2Y) at Siemens in Switzerland. M2Y, an end-to-end music distribution platform, supports several mobile music devices, including Siemens own Digital Music Player (DMP). The DMP is a PDA-like device that allows users to download DRM-protected, full-length music tracks wirelessly or via the Internet directly onto the device without the need for a separate music player. The first in this product family, the Siemens SX1 integrated mobile music phone, made its debut in August.

"If operators want to make money today on music download services, then they have to go with SDC DRM," Panzera says referring to the proprietary DRM technology at the heart of Siemens' M2Y music distribution platform. "We are pragmatic and provide DRM solutions as the market demands them," Panzera continues. "We also support Microsoft DRM and, when the market asks for OMA DRM (2.0), we'll be among the first to support it."

But operators aren't clamoring for standards—they're competing for subscribers. Siemens, for example, has seen a run on its technology by mobile operators including O2 in the U.K. and Germany. "We are talking to a lot of providers who want to integrate with SDC DRM so they can be first to market," Panzera says. Siemens offers the service in a prime Application Service Provider model that minimizes up-front investments and allows Internet and mobile service providers to establish a complete music distribution business.

The SDC DRM technology, provided by Secure Digital Container (SDC), a Swiss DRM company, works without a client installation and runs on all devices that provide Java Virtual Machine. The result is a multi-device DRM approach that allows users to download music once and play it across a range of mobile and fixed network devices, according to SDC COO and cofounder Michael Bornhäusser.

"Looking ahead, super-distribution and multi-device and operating systems portability across fixed and wireless networks is imperative if providers want users to buy into their services," Bornhäusser says. SDC has the endorsement of major content players including BMG, Warner Music, Sony Music, and Universal.

## LET US ENTERTAIN YOU

Once the nightmare of the content owner community, super-distribution is now seen as the business model that can bring fresh ideas—and new revenue streams—to the worldwide recording industry. As of this writing and if tests are successful, EMI is slated to become the first record label to launch a trial of super-distribution, enabling users to send music tracks to others legally. EMI says this is "currently planned for Q1 2005. The trial with an unnamed U.K. mobile operator marks the first serious effort by a music company to cash in on the viral potential of mobile music. The service allows users to send songs to their peers, who will then be able to preview a track several times to decide if they wish to buy it. A DRM wrapper on the content will cause the track to expire and disappear from the device if not purchased within a set time frame.

The download service is being driven jointly by Ted Cohen, EMI Music's SVP for digital development and distribution, and EMI's U.K. Digital Team, headed up by Doug Lucas, VP, business development. Widely regarded as the "pope of digital music," Cohen admits no DRM scheme is bulletproof, but that's no reason

## DRM's Hidden Value

Digital watermarking is not only a means to prevent copyright infringement. In the mobile space it is gaining traction as a technology to link content and commerce together.

Camera phones—mobile devices that now outnumber cameras worldwide in sales—can "read" a digital watermark from any printed material. "The user can use a mobile to navigate all the information connected to a particular piece of content," explains Ken Levy, director of technology and market development at Digimarc Corp., a provider of secure media solutions. But it goes well beyond that, he says. With Digimarc's technology, companies can invisibly enable any printed content with a link, creating a one-click digital gateway to ecommerce, he says. To develop applications based on this technology, Digimarc is working with companies in the mobile space including Intel.

In the case of a movie poster, for example, the digital watermark can link a mobile phone user with movie times, trivia quizzes, and even a mobile video trailer of the film. And, if users want, they can also buy movie tickets, t-shirts and even a CD of the soundtrack. "The benefits of digital watermarking go beyond content protection. We can help deliver brands gains in value and customer loyalty."

Digimarc's digital watermarking technology provides a persistent digital identity for various media content and supports media rights management applications. The company also provides detection with forensic tracking that allows content companies to secure what Levy calls the "analog hole." Watermarking is woven into the fabric of the content. Because it survives digital to analog conversions, it is user friendly, Levy says. "Legacy devices work. You can watch a DVD copy on a VCR. Our approach doesn't stop people from using content, it just makes sure the content owners are properly paid."

for content owners to pass up on the opportunity to distribute their content over wireless. “We need to make music available now. If we embrace it early and get people used to paying for [music content] early as well, then we have a business model,” Cohen explains.

He flatly disagrees with restrictive DRM schemes that treat users like potential criminals. “We have to craft consumer behavior, not blunt it,” he argues. “P2P isn’t a bad thing—unless it’s uncompensated.” Unlike many of his peers, Cohen also supports the ability of users to access music content across platforms and devices. “Whether it’s PC to phone, phone to PC, or a mix is irrelevant. When users pay for music content, their experience should be fluid and they should be able to move the music around freely in their ecosystem—as long as that ecosystem isn’t a dormitory or zip code.”

Cohen is currently considering several DRM solutions and approaches to make super-distribution pay off for providers and users. One model would reward users who turn their friends on to music with points that they could trade in for more music—or even cash. “If someone is a music evangelist and spreads the word about how good a certain song is, then he should get something in return,” Cohen says. But no matter what DRM schemes should emerge over the next months, his message to his industry peers remains the same: “Be proactive about mobile and get on board!”


Determined to do battle with its rival, i-Pod, the SX1 is Siemens’ flagship multimedia device. Designed for consumers who want to make the most of 2.5G services like video MMS and over-the-air (OTA) downloads of applications and content, the feature-packed device includes a built-in video player, camcorder, music player, and FM radio as well as a 64K color high-resolution screen.

## TAKING CARE OF BUSINESS

While mobile entertainment companies have made significant progress toward providing users with a seamless DRM scheme that will allow content access anywhere, anytime, and on any device, the mobile enterprise has a long way to go. Like DRM in the mobile entertainment space, enterprise DRM lacks standards. This means that content protected by one set of software cannot be easily played, watched, or read via a device or application that supports a different set of technologies. This wasn’t an issue when the workforce was tied to PCs and concerned only with the management of content distributed *within* the company.

However, no company is an island. It is connected and must, therefore, share its DRM-protected content—with partners, suppliers, shareholders, and stakeholders. To complicate matters, a large proportion of the enterprise workforce is mobile and requires the ability to read, change, forward, and redistribute content on the fly.

To date, limitations such as screen size and memory make it difficult for remote workers to access—let alone interact with—content on mobile devices. But, as Erica Rugullies, a senior analyst at Forrester Research, points out, this hurdle is being overcome. “We see more of it in the healthcare profession, where the use of handhelds among doctors to view images such as x-rays is growing,” Rugullies says.


An additional driver is HIPAA, the Health Insurance Portability & Accountability Act, which requires that personal health information be stored in a proper manner and guarded against improper use. The privacy of patient records extends across devices, so the industry will need DRM solutions that extend across those devices as well, she adds. “But the mobile technology capabilities aren’t there yet,” she says. “When the technology reaches this point, then we’ll see DRM solutions emerge to protect that content.”

Authentica Inc., a provider of enterprise DRM (E-DRM) solutions, has recently completed a study of current and future customer requirements for E-DRM systems. Customer feedback underlines the desire to have the same control over email, whether it’s viewed on a PC or on a BlackBerry, Victor DeMarines, director of marketing and product management at Authentica, says. “Customers that have an email retention policy of 60 days, for example, want that email to expire at all the different points the email touches.” For this reason, Authentica has placed mobile DRM on its product roadmap for next year. “We want to extend secure viewing to the BlackBerry as it becomes more of a requirement [from our customers].”

Authentica has seen customer interest in E-DRM solutions surge this year, according to DeMarines. “Companies—particularly in the manufacturing and government sectors—can’t just use their perimeter security technology to protect their data. They must increasingly share data across different nodes and devices, and so mobile is becoming a key part of their total E-DRM strategy.”

SealedMedia, another leading provider of document security solutions, is also convinced mobile is an important part of the product roadmap moving forward. “Many of our customers would like secure documents to open up on devices such as BlackBerry,” notes Alan Cornwell, the company’s COO.

## CLEARING DESKTOP CHAOS

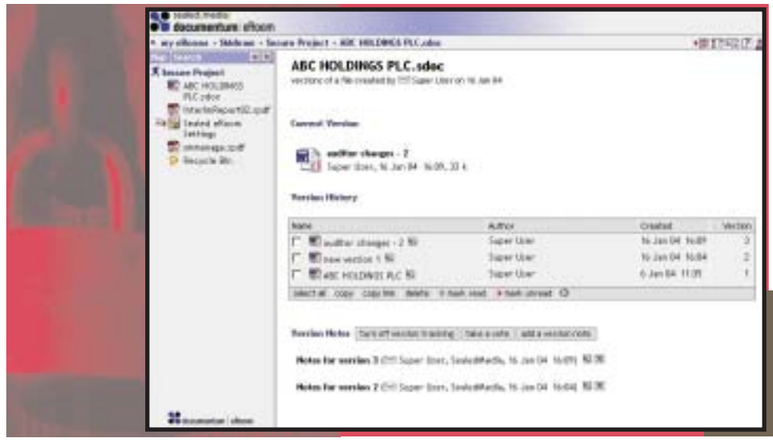
As Cornwell sees it, most E-DRM products work according to what he calls the “M&M” principle. “The ‘M&M’ approach to security relates to the hard perimeter reinforcement and relatively soft-in-the-center strategy adopted by most organizations. Firewalls and other solutions are aimed at building a wall, or a hard outer shell, to protect the enterprise from itself and the outside world,” he says. “A hard shell is too confining to enterprises today to achieve information security so a new approach is required.” Remote workers armed with laptops and PDAs want to work outside the walls of the enterprise. “So the problem becomes not how do we protect the enterprise,” he says, “but much more how do we protect information when it’s external?”

Many E-DRM solutions try to keep all content in a secure repository. But, Cornwell argues, remote workers also create confidential content on their laptops and PDAs in the form of emails, Word documents, and PowerPoint presentations. “What we therefore need is a product that is complementary to a content management system and controls this chaos on the desktop,” he says. To this end, SealedMedia has teamed up with partners including Documentum to extend its security and tracking capabilities past the repository to the desktop, providing rich document security and control capabilities to new and existing business processes.

Indeed, mobility is a key focus for Xansa, an international business process and IT services company with delivery capacity in India. It relies on SealedMedia solutions to secure the company’s so-called Method abc, a delivery framework that spans the complete service cycle from proof-of-concept to continuous improvement and service measurement.

Every six months, thousands of copies of Method abc are produced and distributed via CD-ROM and an extranet for Xansa consultants to use in their work with clients. Previously, Xansa encrypted the CDs, but still risked losing control of the documents once the CD had been unlocked. Today SealedMedia E-DRM technology effectively allows Xansa staff to convert and seal documents on the fly. To ensure that consultants always have the latest version, these licenses are refreshed monthly when consultants collect email and submit time sheets.

“The very essence of our delivery system is tied up in mobility,” notes Paul Weston, Xansa service manager in charge of Method abc. “When work with a particular client is over, the consultant can depart with the confidence that he is not leaving Xansa’s intellectual property behind to be reused…When we walk out, so does our CD.”




While Documentum eRoom enables knowledge workers to plan and execute project work and collaborate with extended enterprise teams, SealedMedia ensures that digital information remains persistently protected within the eRoom itself and when files are viewed or edited on remote desktops.

## LOOK, DON’T TOUCH

CYA Technologies, Inc, provider of business continuity and secure collaboration software solutions, takes a different approach to DRM: Users share the information, not the files. Put simply, the information stays in the repository.

“We designed our software opposite of the rest of the industry. Most of the DRM technology focuses at the desktop level and we believe that—if someone wants to hack the system—the desktop can never be a secure environment unless the information never lands there,” explains Elaine Price, the company’s CEO and co-founder. “With our technology you can see [the information], but you can’t touch it. You can collaborate back and forth, but we have total control over the information to the point that we can dynamically retract the right to access, if the customer requires.”

While mobile isn’t currently the top priority on the CYA product roadmap, Price says the technology can “easily support a wireless environment when the customer requires this capability.” In a scenario involving a BlackBerry device, for example, the user would receive a link via the BlackBerry that would allow the user to view the content on that device or any other. “We pass the key to the user via email, so we invite the user to come to us and access the information in our repository,” Price explains. “As long as the user has email and is online we can reach him.”

If the user requires the information and not a copy, then CYA’s next software release will allow this and warn users when their information is outside the security of the repository.

### Companies Featured in This Article

| | | |
|---|---|---|
| Amplefuture www.amplefuture.com | Digimarc Corp. www.digimarc.com | Ovum www.ovum.com |
| Authentica, Inc. www.authentica.com | Electronic Frontier Foundation www.eff.org | SealedMedia www.sealedmedia.com |
| Beep Science www.beepscience.no | Forrester Research www.forrester.com | Secure Digital Container (SDC) www.digicont.ch |
| Capgemini www.capgemini.com | Open Mobile Alliance (OMA) www.openmobilealliance.org | Siemens www.siemens.com |
| CYA Technologies www.cya.com | | TeliaSonera www.teliasonera.com |

The CYA Secure Collaboration Platform allows organizations to collaborate and share information while controlling actions such as printing, saving, emailing, and cutting and pasting content into other documents. The platform clarifies how information is used since organizations exchanges only links to the information and never the actual file.


Bayer Healthcare AG, a division of Bayer AG, the German pharmaceutical company based in Leverkusen, is currently testing E-DRM solutions, including the technology provided by CYA. "DRM solutions can allow us to maintain the integrity and confidentiality of our internal data and protect our intellectual property position, particularly in the exchanges that take place between lawyers as they iron out the details of a contract," explains Lars Johannsen at Bayer HealthCare AG.

While Bayer Healthcare Research and Development is not currently "pursuing a strategy to becoming a mobile enterprise," Johannsen says mobility increasingly plays a role in business scenarios. "We don't currently provide options for staff to pull content from our repositories with mobile devices, but the technology would allow remote workers to access information from their laptops or PDAs from the external sites such as airports." Mobility, he adds, will be an important requirement for DRM solutions moving forward.

**DO YOU WANT TO KNOW A SECRET?**

While companies fine-tune their DRM technology and solutions to meet the user demand for anywhere, anytime, and any-device access, Cory Doctorow, a science fiction writer and a vocal member of the Electronic Frontier Foundation, a non-profit membership organization that works to uphold civil liberties interests in technology and standards, argues that all DRM systems are ultimately bad for business—and society. He distrusts E-DRM solutions and their promise to maintain the integrity of content. "DRM systems are only as good as the people who use them," he says. "The idea that we can substitute technology for accountability is patently wrong." While it might give patients a secure feeling to know legislation such as HIPPA restricts hospitals from improper use of patient records, no technology can make doctors and nurses honest. "The fact that medical personnel can't forward information doesn't say whether your secret is safe with them," he says. "DRM doesn't make your information secure—only accountability and regulation can accomplish that."

He further points out that E-DRM systems implemented to enforce compliance with the Sarbanes-Oxley Act of 2002, might actually be tools in the construct of future cover-ups. "Since no E-DRM solution can stop the leaking of information, the only plausible scenario for DRM here would be to hide malfeasances, not prevent them."

Doctorow's opinion of the business value of DRM in mobile entertainment is equally low. For one, in all DRM scenarios the "attacker is also the recipient," Doctorow explains. "At the end of the day, all DRM systems share a common vulnerability: they provide their attackers with ciphertext, the cipher and the key. At this point, no secret is a secret anymore."

It's also "absurd" to seek content owner consensus on DRM systems in the first place, he argues. "We've never cared that advances in devices such as television and radio evoke a panic response in entertainment companies. Now we worry about providing entertainment companies with assurances that their content isn't being used against their wishes."

And who defines what's in the interest of content companies? Content companies. Doctorow posits: "If you buy an alarm clock that plays CDs, would someone complain that you are pirating a provider's alarm tone business? Of course not. So why do we go to the media companies and ask them before we create features for our mobile phones?" Ironically, even if the industry does succeed in meeting requirements for DRM systems, many users won't buy them. "The business model is flawed," Doctorow says.

The arguments in favor of DRM remind him of the get-rich-quick plan presented by the underwear-stealing gnomes in the popular animated series *South Park*: In one episode, gnomes that steal underwear appear in *South Park*. When confronted with their crime, they reveal they have a three-step plan to make money from the underwear. One: steal the underwear, two: (silence), and three: get rich. "It's the same way in the mobile space," Doctorow muses. "One: equip all devices with DRM controls and feud about interoperability, two: (silence), and three: content providers get rich." There's no silver bullet solution for DRM, he says and claims there ever will be are wishful thinking. E

**PEGGY ANNE SALZ** (peggy.salz@gmx.net), a freelance technology writer and author based in Europe, tracks not only the global mobile telecom industry, but also the business models and trends that will shape its future. Comments? Email letters to the editor to ecletters@infotoday.com.