VENABLE LLP

THE DOWNLOAD

DEVELOPMENTS IN E-COMMERCE, PRIVACY, MARKETING, AND INFORMATION SERVICES LAW AND POLICY

VOLUME 1, NUMBER 1 NOVEMBER 10, 2006

EDITORS

ALISA M. BERGMAN
202-344-4611
abergman@venable.com

EMILIO W. CIVIDANES
202-344-4414
ecividanes@venable.com

STUART P. INGIS
202-344-4613
singis@venable.com

■

WASHINGTON, D.C.
575 7th Street, NW
Washington, DC 20004-1601
(202) 344-4000

BALTIMORE
Two Hopkins Plaza
Baltimore, MD 21201
(410) 244-7400

ROCKVILLE
One Church Street
Fifth Floor
Rockville, MD 20850
(301) 217-5600

TOWSON
210 Allegheny Avenue
Towson, MD 21204
(410) 494-6200

TYSONS
8010 Towers Crescent Drive
Vienna, VA 22182
(703) 760-1600

NEW YORK
405 Lexington Avenue
New York, NY 10174
(212) 307-5500

LOS ANGELES
2049 Century Park East
Los Angeles, CA 90067
(310) 229-9900

Welcome to the inaugural issue of Venable's THE DOWNLOAD—a periodic newsletter highlighting breaking developments in e-commerce, privacy, marketing, and information services law and policy. In the past two years, Venable has enhanced its practice areas with the additions of Milo Cividanes, Alisa Bergman, Stu Ingis, Will Nordwind, and Kay Pauley, all leading practitioners in the law and policy of privacy, data security, and Internet marketing. These additions complement Venable's long-standing premiere consumer protection, advertising, and marketing practice areas.

FTC Holds Hearings on Next 10 Years of Consumer Protection

The Federal Trade Commission this week held three full days of hearings on "Protecting Consumers in the Next Tech-ade," to "examine the key technological and business developments that will shape consumers' core experiences in the coming 10 years." These hearings built on the hearings held in 1995, at the inception of the commercial Internet, which helped the Commission set its consumer protection agenda of the last 10 years. The hearings also provided interesting descriptions of emerging technologies and associated policy issues. The sessions covered a broad range of issues from social networking sites, to user-generated content, the future of marketing and advertising, RFID, convergence, and payment systems and devices, with remarks and discussions by all of the FTC Commissioners and representatives of businesses, leading trade associations, and consumer advocate groups.

Drawing on lessons from the past, FTC Chairman Majoras highlighted the importance of competition in the marketplace, noting that it is critical to consumer welfare. She also spoke about the adaptability of FTC legal standards, noting that "carefully adapting existing legal standards ensures that we can keep up with new consumer protection problems and decreases the risk that new laws for new technologies will create unintended negative consequences." Finally, the Chairman spoke about the relationship between technology and consumer expectations, stating that technological change has altered consumer behavior, and with these alterations come an increase in consumer expectations, to which "[c]onsumer protection policy must be prepared to respond."

The following is a chronological summary of the November 6-8 hearings.

MONDAY, NOVEMBER 6, 2006

MONDAY, NOVEMBER 6, 2006

FTC Chairman Deborah Platt Majoras, in her opening remarks, noted the difficulty of creating public policy given the rapidly changing nature of technology and its effect on the way we live. These hearings are a primary feature of the FTC's response. The focus is not on the changing technology itself, but its impact on consumers and the appropriate policy response for the government to take in protecting them.

These hearings build on earlier efforts, most notably the hearings led by Chairman Pitofsky in 1995, known as the "Global Hearings," which focused on the same issue. The Global Hearings introduced the FTC's policy agenda for the decade in this area, as the FTC hopes to do at these hearings. The previous hearings predicted many of the privacy and security issues that have emerged since then.

Chairman Majoras identified four lessons from the past: 1) technological change is notoriously difficult to predict; 2) vigorous competition is necessary to enhance consumer welfare; 3) FTC goals can often be accomplished with existing law (in 1996, for example, no one was even talking about spyware, but existing FTC authority has enabled it to combat this threat effectively; when Congress provides new tools, the FTC vigorously uses them, *e.g.*, the CAN-SPAM Act); and 4) technological advances have the effect of increasing consumer expectations. Consumers want their risks minimized, but they do not want any reduction in convenience or choice.

I. Key Changes Predicted in the Next Tech-ade

Frederick Hollman of the **U.S. Census Bureau** highlighted relevant demographic trends, such as the overall aging of the population. **Joseph Bates** of the **Consumer Electronics Association** (CEA) predicted that time-shifting and place-shifting will continue to grow in importance as consumers exert greater control. Consumers want more of their devices connected to the Internet, including appliances. Mobile technology will continue to be a focus, including Internet access and entertainment in the automotive setting, location-based services, wireless broadband, and payment using RFID and mobile phones. The CEA believes that the role of government is to protect consumers' fair use of lawfully acquired content. As consumers' control increases, advertisers may need to change their business model, and live television may become a thing of the past.

Alan Schulman of **Brand New World** pointed out that advertisers have shifted from mass marketing to micro marketing, from simply placing a call to one television

network to targeting smaller groups and reaggregating. Early adopters spread both the device adopted and the market for reaching the people who begin to use it. It is not efficient to create a message for a single household, but through cable operators it is possible to reach a small fraction of a ZIP code rather than targeting a whole city. New niche technologies such as podcasting allow advertisers to reach particular audiences, *e.g.*, advertisements targeted to Harley-Davidson fans. Advertisers are figuring out how to reach consumers through new media without being intrusive; for example, using shorter-form messages, advertisements on ATMs, or QR codes replacing UPCs. It can be a disadvantage to advertise on perishable content, such as a nightly TV newscast, and advertisers are turning instead to platforms that will last, such as movies on DVD. Online-based social networks are beginning to rival the family unit in importance as an advertising target, but advertisers have not thus far been able to reach these networks effectively. Search engine spiders enable contextual ad placement without intermediaries, and this may threaten the traditional advertising model.

Fred Cate of the **Center for Applied Cybersecurity Research, Indiana University School of Law** asserted that the notice-and-opt-out model may become obsolete in the context of mobile devices that have no screen. The notice-and-choice model assumes a face-to-face relationship, but in the case of information aggregators there is no such relationship. We do not use notice and choice in other areas – you cannot opt out of other varieties of consumer protection laws. We have been using state and local laws to deal with global data flows and outsourcing, which are inherently international issues. As demonstrated by the EU's Article 25 and British Columbia's effort to block outsourcing, crafting consistent legal solutions will be a challenge. Domestically, the framework of privacy laws is incomplete and incoherent, with too many agencies participating and different laws for each of many technologies. Professor Cate believes that there is too much emphasis on individuals as victims of fraud. Individuals do not use the tools given to them, such as free credit reports and mandatory rectification, and new types of fraud include synthetic identity theft, which has no individual victim.

II. The Changing Internet

FTC Commissioner Jon Leibowitz noted that private sector efforts at self-policing undoubtedly benefit consumers and have the advantage of being international. But government has its own relevance when it comes to consumer protection, especially because it defines what conduct is unacceptable. For example, before state data breach notification laws, many breaches never became public. The FTC lacks authority to take the necessary action against spyware now. On Friday, November 3, the FTC settled with adware distributor Zango, but it can obtain only disgorgement of profits, and Mr. Leibowitz noted that it would be better to be able to publicize the companies that used Zango for advertising. The FTC is beginning a study on net neutrality, which involves complex competition issues that are squarely within the agency's area of interest. Up until now, the Internet has benefited from open competition, but the exertion of telecom and cable companies' market power has the ability to endanger that. **Susannah Fox** of the **Pew Internet and American Life Project** drew attention to the social impact of the Internet, focusing on the fact that some segments of society are not connected.

Dr. Vinton Cerf of **Google**, **Peter Cullen** of **Microsoft**, and **Dr. William Edwards** of **AMD** engaged in a discussion with moderator **Kara Swisher** of the **Wall Street Journal**. Dr. Cerf noted that many people's introduction to the Internet, especially abroad, is through a mobile phone. Mr. Cullen stated that the revolution is progressing from computers, as in PCs, to computing, as in the universe of devices. Interoperability will determine who succeeds. Dr. Edwards described the one-laptop-per-child effort based on simplified and cheap computing technology. Dr. Cerf asserted that diversity of

input, particularly local content, is threatened by media consolidation as in radio and television. The Internet is filling the gap at the moment, but the ability of the last mile provider to interfere with content is a serious threat to this solution.

Albert Cheng of **Disney-ABC Television Group** noted that ABC was the first network to stream its current, full shows over the Internet. They agreed with consumers that a 30-second ad at the beginning of the show was not desirable, and instead they flash the advertiser's logo at the beginning and have three advertising breaks mid-show, which cannot be skipped until 30 seconds have passed (although the viewer can choose to continue to watch after that). Business partners, such as physical-space retailers, have sometimes objected to online distribution of shows, but ABC/Disney refuses to hold its content hostage to obsolete distribution methods. **Safa Rashtchy** of **PiperJaffray** spoke briefly in regard to financial factors, noting that traditional retailers have come online much more quickly than he expected, which draws sales away from Internet companies like eBay.

III. How Will We Communicate in the Next Tech-ade?

Dana J. Lesemann of **Stroz Friedberg** stated that one trend for the future will be an increased emphasis on strong authentication and encryption as both an offensive and defensive means of protecting communications networks. In the future, she said, when any computer will have instant access to networks, computer forensics will become increasingly difficult as traditional wired servers and networks disappear; therefore, there will be an emphasis on self-protection. She added that one question will be whether, as a matter of public policy, technology companies should keep large amounts of data; storing large amounts of data may aid some law enforcement investigations, but could greatly increase the costs of doing business.

Ari Schwartz of the **Center for Democracy and Technology** focused on the consumer perspective. He said that the goal used to be convergence; however, this goal has been achieved with devices like cell phones that can not only call, but send text messages, record video, play digital music, and view websites; the new goal will be to sync electronic devices together, which will create questions about how to make different devices compatible and how to secure data that is available on multiple devices. He also noted that consumer perceptions of "personally identifiable information" are changing: whereas it used to mean name, address, and/or Social Security number, it now includes anything that could potentially trace back to the consumer (such as a list of search strings).

Dave Cole of **Symantec** stated that instant messaging ("IM") devices and programs are the likely next target of malicious attacks; peer-to-peer (P2P) networks also are becoming a source ripe for attack. However, he said, the nature of attacks is likely to change: instead of viruses or spyware on individual systems, attackers are likely to circulate threats through a network and cancel or tremendously slow down network access. He added that, as technology advances to protect hardware and software, attacks will focus on duping people using techniques like phishing and pretexting; therefore, future efforts to counter attackers will include consumer education.

IV. Social Networking—Trends and Implications for the Future

FTC Commissioner Pamela Jones Harbour spoke about the FTC's efforts to protects children through consumer education and targeted law enforcement. She predicted that, in the future, sites will increasingly use hardware and software verification tools to ensure that users are above a minimum age. Also, she encouraged sites to use a global icon to report abuses to law enforcement.

Benjamin Sun of **Community Connect** stated that social networking sites (SNS) increasingly will target real world communities and their real world needs. **Chris Kelly** of **Facebook** said that SNS will continue their efforts to avoid anonymity; SNS are a "social utility" that help people share information and resources with other members of their communities. **Hemanshu Nigam** of **Fox Interactive Media** (parent of **MySpace**) said that large SNS such as MySpace are aiming to become a worldwide lifestyle brand and a global marketing platform; the ultimate goal is "lifestyle convergence" so that people can do everything in their online world that they can do in the real world. He noted that, in the future, consumer education efforts will result in a consumer base that will innately understand online safety and will automatically expect safety protocols from every SNS. **Andrew Weinreich** of **MeetMoi LLC** stated that the future of SNS is in mobile devices; the interoperability of network carriers, adoption of SMS protocols, micropayments, and worldwide adoption of location-based services will drive a movement toward mobile devices. He added that identity can be authenticated and validated easily by device.

danah boyd of the **School of Information, University of California, Berkeley** noted that older populations went to SNS to meet new people, whereas younger populations go online as a means of establishing a "hang out" place within the public sphere. She stated that four issues will shape SNS in the future: (1) persistence—what is written online often stays online in some form; (2) searchability—children online cannot hide from parents, marketers, or predators; (3) replicability—copying and pasting information; (4) invisible audiences—people speak differently depending upon their audience, and SNS do not necessarily permit the speaker to "see" their audience and adjust their speech accordingly.

Anne Collier of **Net Family News** noted that "live world" video games will grow alongside SNS as a means of establishing community in the future. She noted that basic online safety tips generally do not apply to SNS—most children will not find predators or pornographic images while on SNS unless the children are actively seeking them; therefore, the children who are most at risk online are the same children who are at risk in the real world. She stated that the goal will be to identify these children and work with their parents through collaborative processes to reduce the child's risky behaviors. She added that online safety will not be about technology; it will be about parents communicating and partnering with their children.

V. User-Generated Content—What Does it Mean for Consumers & Marketers?

Amanda Lenhart of the **Pew Internet and American Life Project** offered various statistics regarding online consumer behavior and the creation of online content. She also noted that "user-generated content" includes a broad variety of activities, including text, audio, video, programs, applications, and games. **Andy Chen** of **PowerReviews.com** noted that, for product review sites, it is helpful if one person does multiple reviews, yet a trail of reviews can reveal personal information. He noted that some reviewers want to be high-volume reviewers and seek that reputation; by contrast, other reviewers who want to be critical often value anonymity. He stated that it is often

best to let the consumer choose whether he wants to be identified (even by nickname) or remain anonymous. **Mack Tilling** of **Vizu** noted that there is a similar issue for sites that create polls and ask for comments on polls—a company can learn a lot about a person simply by seeing how they vote on a variety of issues.

Dr. Michael Geist of the **University of Ottawa** noted that consumers produce a significant amount of content, and this content is worthy of protection; consumers' right to speak out should be protected, but many corporate tools are being used against consumers—for example, the ICANN domain name dispute resolution process is being used to prevent, "[brand name here] sucks.com" web sites. In the future, he said, the FTC's role will expand to encompass net neutrality (to prevent consumer-generated content from being relegated to the publicly undesirable "slow lane") and possibly even copyright because overly restrictive use of copyright could prevent fair competition by content-generating consumers against mass corporations.

Jane Kaufman Winn of the **Shidler Center for Law, Commerce & Technology at the University of Washington School of Law** gave a brief presentation on what happens to the consumer landscape when consumers are not simply passive "consumers" of mass produced products, and how the FTC can protect these active "consumers." She noted that the FTC can police deceptive practices, such as a marketing masquerading as user-generated content or a marketer hiring people to draft product reviews. She also said that the FTC could support the industry creation of self-regulatory programs and increasingly transparent practices.

The panel then addressed the question of data mining, and concluded that few companies are currently data mining; every site has bits of information about a person and a problem will only arise when a company can capture all these bits of information across multiple sites to form composite profiles. Mr. Chen noted that, although a company could create a "bot" to troll sites and pick up these bits of data, consumers are savvy to data privacy practices. With increased transparency, clear privacy disclosures, and SNS, news of undesirable practices will spread quickly and then consumers will regulate their own behavior—they will either opt out or will stop visiting the offending site.

TUESDAY, NOVEMBER 7, 2006

I. Benefits to Consumers of Living in an Instant Information Culture

This panel featured case studies of products and services that enable consumers to undertake product comparisons and make purchases online in the areas of retail, buying a home, and shopping for a car. On retail behavior, Kamran Pourzanjani of **Pricegrabber.com** reported that 25-30% of Internet users take advantage of comparison shopping to save time and money. He added that 70% of consumers do not purchase products based on lowest price; factors such as brand name, store/site name, store policies, and customer service also are considered. Mark Chandler of **Autoland,** the largest credit union auto-buying service, described his site, which enables car buying and selling and facilitates research. He said that his site takes some of the risk out of consumers selling their own cars, and helps consumers with the entire car buying process.

Liam Lavery of **Zillow.com** discussed purchases of real estate online, noting that few people actually purchase homes online. He said that the Zillow site offers satellite views, using public record data, among other data, as a key source of information about homes. He added that, realizing that public record data is not always accurate, in response to consumer suggestions, Zillow now allows users to correct

inaccurate data about their homes. Noting that the site is primarily advertising supported, he stated that if you get consumer information right, you can put contextual information around the sides.

Jeff Fox of **ConsumerReports.org** described the ways in which the site provides information about various products: magazine features, reviews and ratings, blogs, message boards, daily news, and interactive tools. He said that consumers are increasingly turning to blogs, online communities, and other user-generated content for product reviews. He noted, however, that such user-generated content has not replaced branded media reviews—these still play an important role in consumer decision making. Mr. Fox also noted the importance of accurate, real-time information.

Information from **Forrester Research** presented by Lee Rainie of the Pew Internet & American Life Project indicates that there is an increasing trend of doing online research before purchasing products; given the vast quantity of information available, some consumers research extensively online and then attempt to triangulate findings. She said that many consumers research online, but still make the purchases offline. The amount of information available online has grown in volume, but consumer attention is short; consumers turn to social networks to help make sense of this information.

II. Marketing and Advertising in the Next Tech-ade

In his opening remarks, **FTC Commissioner J. Thomas Rosch** noted that in the 1970s privacy and data security were "not even on the horizon," adding that, even in the mid-1990s, "the Commission didn't see coming a number of things that affected consumers and their welfare," such as spyware and spam. He said that the Commission underestimated the way in which people would come to create and share content though blogs, message boards, and social networking, and noted that innovations come with price tags, in the form of, e.g., privacy and copyright issues.

Commissioner Rosch stated that identifying the relevant technologies is important to future consumer protection efforts. He noted that broadband and high-speed Internet access will propel us into the future, with RFID and wireless technologies playing key roles. Looking to the future, he noted that viral marketing and the increasing participation of teens and children in these activities will be an area to watch, particularly as parents are less familiar with new technologies.

Behavioral Targeting and Other Search Trends

Dave Morgan of **TACODA** noted that the place, time, and method of consuming information will change, and it will be possible to better determine what information is delivered and the reaction to it. He added that there will be more information available to more people and a greater dependence on advertising, and noted that industry is taking more affirmative steps to address issues raised by increased behavioral targeting, including adopting of the Network Advertising Initiative (NAI) guidelines and good practices and guidelines on notice about and use of anonymous information, as well as additional disclosures about use of cookies.

Jennifer Barrett of **Acxiom** discussed Acxiom's targeted marketing and the products they provide to their customers, as well as the importance of notice and choice. She stated that clients combine their own data with third-party data to enable more efficient marketing and more relevant consumer offers. She noted the dynamics of the online space, highlighting the importance of respecting users' ability to remain

anonymous. She discussed the importance of consumer trust, noting that data collected should be appropriate to the use for which it is put, and that there should be notice and choice about sharing and security. She also noted that the Direct Marketing Association and NAI have mandatory codes of conduct. She said that those advertisers who will succeed will be those who respect consumers, provide choice, respect anonymity, and safeguard data.

In general discussion, it was noted that the Internet provides the ability to better target as well as more accurately and more quickly measure response than other means of advertisement. Ms. Barrett stated that there is an increased use of statistical analysis. **John Greco**, President of the **Direct Marketing Association**, said that all marketing is moving to direct marketing, discussing "the power of direct." Mr. Greco described the benefits to consumers from leading brands that compose the DMA membership. He noted the need for advertising to be relevant, responsible, and provide results. To be relevant, Mr. Greco said, analytic capability will need to increase.

Marcia Hofmann of the **Electronic Frontier Foundation** stated that consumers are concerned about privacy and want to maintain control. She agreed that people want relevant ads; however, consumers should be able to choose what sorts of ads they would like to see. Mr. Greco stated that it will be important to carefully look at the situation to determine what type of choice makes sense. Noting the title of the hearings, Mr. Greco stated that to protect consumers, we need to determine from what we want to protect them beyond the areas upon which everyone agrees. The first point of focus should be where there is consensus of harm in areas such as identity theft, fraud, and child exploitation. He added that if consumers are not presented with advertisements, there may be missed opportunities. Mr. Greco also emphasized that in the complexity of the information age the types of choice will be diverse and numerous.

Mobile Content and Marketing in the Next Tech-ade

Brian Stoller of **Third Screen Media** discussed the high volume of mobile penetration and the important role that carriers play in turning off unwanted advertising targeted to mobile phones. He noted that advertising will benefit the mobile world and will subsidize content—people who access Web content through their mobile phone end up paying more in subscription fees; if advertising is allowed, subscription fees will go down.

In general discussion of wireless marketing, it was noted that what is key to advertising success is not being intrusive. Mobile Marketing Association (MMA) and Interactive Advertising Bureau (IAB) are establishing standards for advertising on phones. Ms. Hofmann noted that the vast majority of consumers will have problems with marketing that intrude into their space. Mr. Greco stated that if we are talking about some form of mobile service, one way or another people have expressed a desire to participate. He said that when new technologies are introduced, we need to understand them and the consumer issues they pose and then adapt accordingly.

The Interactive Future

Brian Wieser of **MAGNA Global USA** stated that there is a great deal of data indicating that consumers are taking control, but noted that consumer control on a widespread basis is constrained. He also stated that early adopters of technology are not necessarily representative of consumers and their desires, and that changes in behavior

only occur when perceived crisis outweighs the pain of adoption. Mr. Wieser also noted that conventional TV has outpaced online on-demand. Mr. Greco noted that, in thinking of the future and advertising in the various mediums, we need to consider business models, the ease of use of technology, and age groups—something programmed into someone's life versus something they are converted into.

Mr. Wieser said that he continues to explore whether consumers want control; the "utility of choice," he said, is that we tend to value things "based on the opportunity costs lost." He noted that choice is not inherently appealing to consumers, and it is often overwhelming unless the other option seems more inconvenient. Mr. Morgan stated that people love to have choices, and this fact is not captured by some of the statistics. Ms. Barrett stated that consumers want choice, but they want choice that they can understand; choices that are too complex can create paralysis.

III. Computing Power and How it Will be Used in the Marketplace of the Next Tech-ade

Dr. Eric Horvitz of **Microsoft Research** discussed current and projected developments in artificial intelligence (AI); advertisers, for example, will benefit from models that more accurately calculate clickthrough likelihood. He said that personal data such as previous driving routes and destinations, or web search criteria, will exist within a "shroud of privacy." Moderator **Dr. Mark Bregman** of **Symantec** stated that there will be commercial pressure to open the shroud and use the consumer information collected. Dr. Horvitz noted that there are solutions such as using only aggregate data, but he acknowledged that features of the marketplace will make it difficult to protect individuals.

Dr. Anthony LaMarca of **Intel Research Seattle** provided an introduction to sensor networks, which he defined as computer networks of spatially distributed devices used to monitor surrounding conditions; examples include the sensors spread around a modern car or measurement devices scattered in the path of a wildfire. He stated that sensor networks raise their own security challenges, as more computing elements means there is more to secure, and the radio networks used for transmission are easier to intercept than communications over wires; responses include encryption and reliable authentication, which is stronger on sensor networks than on most computers, since each sensor can verify a transmitter's identity by checking against another nearby sensor. Dr. Bregman asked about the possibility of spoofing sensors or simply avoiding them. Dr. LaMarca explained that systematic avoidance of sensor networks exists already, in the form of web sites showing drivers how to get somewhere while appearing on camera as few times as possible, for example.

Sal Capizzi of **Yankee Group** assessed the impact of data storage growth, noting that larger storage capacity makes it easier to work on a mobile device, which leads to more opportunity for data breaches through theft and interception. **David Hitz** of **Network Appliance** contended that state data breach laws are a good start, but that the state-by-state approach is difficult for corporations trying to comply with all of the laws at once. He argued that Congress needs to provide a uniform national law both for the protection of consumers and to provide some consistency to regulated entities.

Dr. B.J. Fogg of **Stanford University Persuasive Technology Lab** described the potential for use of persuasion profiles in advertising. He said that systems will record which strategies effectively persuade an individual, and this data will be sold for use in the market and in settings such as political campaigns. **Deirdre Mulligan** of the **Samuelson Law, Technology & Public Policy Clinic at the U.C. Berkeley Boalt Hall School of Law** cited state laws restricting radio frequency identification (RFID) as an example of the failure to combat fears of technology. She stated that industry and government can avoid results of this nature by educating people and developing best practices preemptively, before the technology becomes widely used.

IV. RFID Technology in the Next Tech-ade

Joshua Smith of **Intel Research Seattle** described projects using RFID for activity monitoring in caring for the elderly, and for activity assistance using RFID-enhanced robotics. **Richard Adler** of the **Institute for the Future** described the potential for RFID to transform health care from periodic monitoring during occasional hospital visits to monitoring anywhere, at all times.

Jeroen Terstegge of **Royal Philips** described the potential for RFID use in the home, where it will be embedded in appliances and robotics to take care of ordinary tasks. **David Turner** of **Microsoft** discussed near field communication (NFC), which operates at a much shorter range than RFID; in NFC applications such as contactless payment cards, limited range is the advantage: the user gains an intuitive selectivity with regard to connections, a directed approach. He noted that interoperability is a tremendous challenge, and said that Microsoft is investing in both NFC and traditional RFID.

Sandra Hughes of **Procter & Gamble** discussed the electronic product code (EPC) application of RFID. She explained that EPC can counteract inefficiencies in the supply chain, where out-of-stock items would otherwise lead to lost sales; today, EPC is widely used only at the level of tagging pallets and cases, rather than individual items. She said that P&G uses it to ensure that display cases are properly located, *e.g.*, keeping batteries next to battery-powered razors; P&G also uses EPC for products that are the most frequent targets of shoplifting, such as tooth-whitening strips. She noted that standards organization EPC Global is working on privacy issues that will accompany the expansion of EPC to the individual item level, including consumer education and implementing notice-and-choice procedures.

Paul Moskowitz of **IBM T.J. Watson Research Center** emphasized that adding EPC to individual items will be slow, but that the advantages would be significant; for example, at checkout a reader can scan all EPCs at once, instead of having to scan each item individually. He said that EPC Global recognizes the security concerns posed by RFID, including the fact that it can be read at a distance of 30 feet and that it uses radio transmissions, and is evaluating responses, including a "kill" command that stops the tag from working after the point of sale; blocker tags that interfere with normal reading; clipped tags, which are enclosed in a metal-lined bag that limits their range to around two inches; mechanical techniques such as destroying the tag; and encryption.

V. Convergence and What it Means for the Coming Tech-ade

Jim Kohlenberger of the **VON Coalition** observed that the separation of media such as voice and video into their own distinct silos is ending, as they become integrated on the web. Moderator **Gregory Sidak** of the **Georgetown University Law Center** suggested using models from antitrust law to overcome the remnants of the FCC's silo approach. **Dan Brenner** of the **National Cable & Telecommunications Association** cautioned that competition and laissez faire approaches can provide a partial solution, but the government needs to prohibit some practices, such as blocking access to a competitor's network entirely. **Taylor Reynolds** of the **Organization for Economic Cooperation and Development** noted that this practice of network blocking is already taking place in Korea, and the negative results should serve as a warning to U.S. regulators. Mr. Kohlenberger agreed, observing that Chile and Belize attempted to block VoIP altogether, and stated that international regulatory bodies need to act preemptively to avoid such results.

Fritz Attaway of the **Motion Picture Association of America** and **Gigi Sohn** of **Public Knowledge** engaged in an extended debate with regard to the protection of intellectual property. Mr. Attaway stated that the greatest threat to convergence is free ridership, which decreases supply and increases prices. Ms. Sohn answered that consumers need to be informed of what they are allowed to do with content they purchase, and currently they are not informed of the contours of digital rights management. **Sarah Deutsch** of **Verizon Communications** commented that times have changed—10 years ago, YouTube simply would have been taken down, but now it is allowed to survive and mitigate its copyright violations.

WEDNESDAY, NOVEMBER 8, 2006

I. Changes in Payment Devices and Systems

Moderator **Elliot Burg** of the **Vermont Office of the Attorney General**, gave a brief introduction to modern payment systems. **Dr. Jeanne Hogarth** of the **Federal Reserve Board** discussed the results of a survey on the use of payroll cards, noting that many consumers could use the cards as a money management tool. She also noted that new ATM technologies are being developed that would enable consumers to scan in checks for deposit.

Jean Anne Fox of the **Consumer Federation of America** stated that consumers would have to have confidence in new payment systems, but laws have not kept pace with the proliferation of plastic cards. She pointed out the ways in which federal regulations regarding credit cards differ from those regarding debit cards. **Paul Tomasofsky** of **Two Sparrows Consulting** noted that consumers demand convenience, but may also alter their behaviors to avoid security issues; for example, many consumers have a credit card that they use exclusively for online purchases. Mr. Burg then showed a video that showcased Philips' NFC technology that lets a cell phone be used to pay for products simply by swiping the phone over a scanning device.

Mark MacCarthy of **Visa U.S.A.** stated that the future of payment systems would be contactless payments. He also noted that, as a matter of corporate policy, Visa gives credit, debit, and stored value cards the same protections. Ms. Fox replied that, while generous corporate policies were a good start, consumers would be better

protected if federal laws were to codify these policies and offer a private right of action. **David Turner** of **Microsoft Corporation** and **James Linlor** of **Black Lab Mobile** stated that future payment systems will be mobile. Mr. Linlor discussed how cell phones currently can be used to pay for products using a PIN system over the Visa network; the issue is storage and what information about payments will be stored on the phone itself.

Marc Kirshbaum of **Experian Fraud Solutions** talked about identity theft and stated that authentication methods are moving towards multifactor approaches and fraud scoring models. **Elliott McEntee** of **NACHA** discussed a new banking product called Payment in Private ("PIP"), that would allow customers to make payments online but keep all payment information with their bank so that the third-party retailer will not receive any sensitive information. Mr. Linlor noted that, although biometrics are a popular topic, they are not necessarily the best authentication method. He pointed out that consumers can get a new credit card with a new number, but they cannot get a new fingerprint, should their information be compromised.

II. New Products—New Challenges

FTC Commissioner William Kovacic spoke on the issue of whether the FTC can stay ahead of product developments. He noted that the FTC should use more effort to punish serious fraud, expand cooperation with other consumer protection agencies in America and abroad, and invest in hiring technology experts.

Tom Jacobs of **Sun Microsystems Laboratories** discussed digital rights management ("DRM") services, which range from complex biometrics to watermarks and copy management. He explained that the central tension in discussions about DRM is that security issues are not being explored in an open fashion, yet copyright owners will not use DRM tools that use open source code that is vulnerable to hacking. **Andrew Moss** of **Microsoft** said that DRM is a tool for content owners and is intended to give consumers choices. **James DeLong** of the **Progress & Freedom Foundation** agreed, stating that DRM gives consumers the choice of buying a book to put on a shelf for $30 or buying the right to read the book once for $3.

Moderator **Deirdre Mulligan** of **U.C. Berkeley** provided an overview of the copyright issues surrounding DRM, noting that DRM permits content owners to control how consumers use the content; this is a reverse of traditional roles, where the purchase of content generally permits the consumer to use that content in a broad variety of ways.

Jeannine Kenney of **Consumers Union** pointed out that most consumers do not currently know what DRM is, do not know what the terms of DRM are for any given product, and have virtually no way of finding out. **Corynne McSherry** of the **Electronic Frontier Foundation** agreed that consumers do not understand DRM, and noted that the presence of DRM should be disclosed before consumers make a purchase; otherwise consumers may not expect DRM to be present. She also stated that DRM vendors must provide independent research firms with the ability to reverse engineer DRM to prevent flaws. She used the Sony rootkit install as a case study to show that content owners are not necessarily in the best position to research the security of DRM.

Dr. Urs Gasser of the **University of St. Gallen Switzerland** provided a brief perspective on DRM in Europe. He noted that France has taken a particularly proactive approach to restricting DRM, requiring content owners using DRM to disclose that fact as well as any interoperability limits. He added that, in Europe, DRM may also constitute an unfair consumer contract. **Manuel Mirabal** of the **National Puerto Rican Coalition** discussed the government mandated shift to digital television in 2009, and how the industry has so far failed to notify consumers of the transition. He suggested that the FTC could take a more active role in consumer education about the digital transition to remedy this.

III. Communicating with Consumers in the Next Tech-ade—The Impact of Demographics and Shifting Consumer Attitudes

William Strauss of **LifeCourse Associates** provided an overview of the effects that generational differences will have on consumer experiences in the coming decade. **Beau Brendler** of **Consumers Union** discussed factors affecting whether consumers trust a web site, noting the particular importance of clearly displaying who made the site and how to reach them. **Scott Shipman** of **eBay** stated that trust is not synonymous with perfect security. Instead, he asserted, the key to building trust is to communicate honestly with consumers when security problems inevitably occur.

Solveig Singleton of the **Progress & Freedom Foundation** predicted that regulatory oversight will become much more difficult as transaction volume on the Internet booms and transactions become smaller-scale and more international. She explained that the market assesses the need for trusted institutions based less on what people say than on what they do, *e.g.*, whether they click a button, or which question on a site makes them leave. She stated that the market self-corrects; if a feature is failing, someone will see the opportunity to get consumers what they want. She argued that the model of providing free products supported by advertising is a weak point in this system, since the seller's real customer is the advertiser rather than the consumer, and there is less incentive to be responsive to consumers.

Dr. Helen Nissenbaum of **New York University** proposed a theoretical framework for assessing context in making privacy decisions. **Dr. Joseph Turow** of the **University of Pennsylvania** cited research showing that consumers think "privacy policy" means that a company will not share information with other companies, and they have similarly little understanding of their rights in the marketplace. He stated that consumers think many practices are illegal that are in fact common practice for businesses, and they have practically no awareness of the data mining that takes place. **Chris Hoofnagle** of **U.C. Berkeley Boalt Hall School of Law** added that viewing end-user license agreements (EULAs) as an informed bargain is a fiction, as consumers do not read the terms, rarely understand them if they try, and often regret entering into the transaction once they find out what it means in practice. He warned that unless consumers are given a helping hand, there will be consequences for the entire network—for example, people will contractually bind themselves into using malware, as in the recent Sony rootkit incident. Mr. Hoofnagle stated that people think data sharing is opt-in by default, and he argued that there needs to be a change in the law to reflect that belief. He called for concrete benchmarks to determine whether self-regulation can be effective.

Peter Swire of the **Ohio State University Moritz College of Law** predicted that the shift in congressional control will result in more pressure on the FTC with regard to privacy issues, as Congress begins to exercise its oversight authority

vigorously in this area. Professor Swire stated that Congress may begin to take legislative action in areas previously limited to the states, such as data breach notification laws. **Trevor Hughes** of the **International Association of Privacy Professionals** noted that indicators of trust are relatively easy to perceive in physical stores, but these indicators have not caught up with the new channels of commerce. He stated that privacy professionals will have a part in creating the new indicators of trust.

IV. How to Make Sense of it All—Consumers' Perspective

Jo Reed of **AARP** mentioned an effort to create a federal database covering all varieties of federal benefits, including Medicare. She stated that AARP is concerned about the consequences of a breach of such a database and is encouraging the utmost care in protecting it. **Susan Grant** of the **National Consumers League** stressed that it is crucial for consumers and businesses alike to have clarity in terms of what conduct is legal, and the FTC needs to take the lead in providing this clarification. **Dawn Rivers Baker** of the **MicroEnterprise Journal** commented on the FTC's neglect of micro-businesses, those with five or fewer employees, in designing its policies. **Beau Brendler** of **Consumers Union** called for companies to pledge to deal only with data storage companies that have demonstrated the ability and intent to protect data.
He asserted that trustworthiness certifications have had little resonance with consumers to this point, but it may be possible to salvage them with significant revisions.

Brent Embrey of the **Indiana Office of the Attorney General** stated that there is an opportunity for market participants to build brand loyalty on the Internet by providing genuine protections for consumers. He explained that businesses could distinguish themselves by demonstrating that the information they collect will stay entirely within that entity and be used only for purposes of serving the customer. He argued that businesses that do not move in this direction are on a collision course with the public, which is not yet aware of where its information is going or how it is being used. He stated that it is becoming increasingly difficult for consumers to know how to access government when something goes wrong; as so many transactions cross state lines, it is unclear which state's law enforcement will protect the consumer. He predicted that this problem will intensify as transactions become more international, since state governments have essentially no capacity to handle problems across national borders.

Jerry Berman of the **Center for Democracy and Technology** called for additional hearings to focus in greater depth on particular issues, such as authentication, DRM, and interoperability. He asserted that the FTC has provided this type of in-depth examination and follow-up in other contexts and needs to do so here. He argued that growing privacy problems demonstrate that self-regulation is not enough, and he called for Congress to intervene. He stated that existing statutes are sorely outdated and are of little help in confronting problems related to current technologies. He explained that the FTC can set the foundation for federal legislation by means of the in-depth hearings he proposes. He praised the commercialization of the Internet as the driving force that transformed it from a research network among a handful of scientists into what it is today.

Concluding Remarks

Lydia Parnes of the **FTC** and **Tamás Andrés Molnár** of the **European Commission** closed by discussing the continuing role of regulators in the U.S. and the EU. Mr. Molnár stated that the discussions at these hearings could have taken place in Brussels, where the E.C. is assembling its strategy in this area for the next seven years. Europe, he noted, faces different challenges, as cooperation among market segments must account for 20 languages and national borders. Ms. Parnes stated that European and U.S. perspectives differ with regard to privacy, but the bottom line for the regulators is the same: protecting consumers. She stated that the next step will be for the FTC to carefully review the information provided by participants, and in the near future the FTC will issue a report discussing the implications of what took place during these hearings.

Venable attorneys Alisa Bergman, Leah Nelson, and Chris Diamond contributed to this article.

THE DOWNLOAD is published by the privacy team at the law firm of Venable LLP. Internet address: http://www.venable.com. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations. Copyright Venable LLP 2006.

Issue Editor: Stuart P. Ingis
Associate Editor: Katharine A. Pauley

Questions and comments concerning information in this newsletter should be directed to Stuart Ingis at singis@venable.com.

Please direct requests to be added to the distribution list or address changes to Kay Pauley at kpauley@venable.com.

You are receiving this communication because you are a valued client or friend of Venable LLP.

To **unsubscribe** from this mailing list, reply to this message with REMOVE in the subject line.