Summer 2009

Technology Initiatives In The New Administration

Richard Raysman

Peter Brown

SPRING 2009, 18 MEDIA L. & POL'Y

TECHNOLOGY INITIATIVES IN THE NEW ADMINISTRATION*

by

Richard Raysman**
Peter Brown***

In the months leading up to his inauguration, President Barack Obama, like any modern lawyer, refused to give up his Blackberry (a.k.a., his "Barackberry"), much to the chagrin of aides who stressed that Presidential e-mails were a potential legal and security risk. The problem ultimately was resolved after President Obama was given a smart phone with enhanced security features.

More than any President of recent memory, technology was a key element to President Obama's campaign promises. The new Administration has made numerous statements about how technology will make government more transparent, and how the country's infrastructure requires innovation to move into the new century. This emphasis is echoed by commentators and interest groups such as the Business Software Alliance,[1] which has suggested that information technology and modern advances should be the cornerstone of some of the biggest projects in the coming years, namely, education, health care, the environment and economic stimulus.

---

* A prior version of this piece appeared in the NEW YORK LAW JOURNAL, Feb. 10, 2009, at 3.

** Mr. Raysman is a partner at Holland & Knight, LLP. He holds a B.S. from MIT (1968) and a J.D. from Brooklyn Law School (1973).

*** Mr. Brown is a partner at Baker Hostetler, LLP.

The authors aree co-authors of COMPUTER LAW: DRAFTING AND NEGOTIATING FORMS AND AGREEMENTS (Law Journal Press 1984). Edward A. Pisacreta, Of Counsel at Otterbourg, Steindler, Houston & Rosen, P.C., contributed to the preparation of this article.

[1] "The Business Software Alliance is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace." *See* http://www.bsa.org/GlobalHome.aspx.

This article will discuss several of the major technology-related initiatives of the new Administration, and the legal issues inherent in such proposals.

I
ELECTRONIC HEALTH RECORDS

President Obama has proposed investing $50 billion over the next five years to expand the adoption of healthcare information technologies (IT), including the wide use of electronic medical records. Echoing this promise, The American Recovery and Reinvestment Act (ARRA), the $789 billion economic stimulus bill recently passed by both houses of Congress and signed into law by President Obama, contains appropriations for healthcare IT.[2] Moving from paper-based record keeping to a healthcare IT system may, among other things, reduce medical errors and drive down health care costs resulting from inefficiency and duplicative care. Also, it will purportedly improve public health reporting and the coordination of care and information among hospitals, laboratories, and physician offices via an effective nationwide infrastructure for the secure and authorized exchange of patient information.

However, there are numerous barriers to expanding the use of electronic medical records. First, providers may be reticent to implement healthcare IT systems because upfront costs can run between $25,000 to $45,000 per physician, with cost savings often inuring to health insurers or other entities.[3] Some commentators have suggested that doctors need financial incentives, akin to the higher reimbursement rates given to Medicare doctors to use e-prescriptions, or targeted subsidies to offset the initial investment, similar to an existing New York City Health

[2] The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Title XIII, 132 Stat. 115 (2009).

[3] Laura Landro, *Incentives Push More Doctors to E-Prescribe*, WALL ST. J., Jan. 21, 2009, *available at* http://online.wsj.com/article/SB123249533946000191.html (last visited Mar. 21, 2009).

Department program that encourages physicians to participate in a citywide electronic health project.[4]

Second, healthcare IT systems must be interoperable nationwide to facilitate the seamless sharing of medical records or lab results.[5] In this regard, President Obama previously stated that he wished to make the Veterans Health Administration (VHA) a model in the use of healthcare IT, and, recently, one enhanced version of the VHA's electronic medical records software, known as VistA, was released under the open source Eclipse Public License.[6]

Third, doctors and technicians will require training on any new digitized system to prevent delays and errors. Last, there are outstanding privacy issues concerning electronic medical records, including minimum data security and breach notification standards, a statutory right to consumer privacy of electronic health information (which may or may not preempt certain state privacy laws), clarification of covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[7] to include additional handlers of electronic medical records, and standards for the sharing of health data.[8]

---

[4] Lisa Wangsness, *Letter Highlights Hurdles in Digitizing Health Records*, BOST. GLOBE, Jan. 1, 2009, at A16, *available at* http://www.boston.com/news/nation/articles/2009/01/01/letter_highlights_hurdles_in_digitizing_health_records/ (last visited Mar. 21, 2009). *See also* Anemona Hartocollis, *City to Pay Doctors to Contribute to Database*, N.Y. TIMES, Dec. 29, 2008, *available at* http://www.nytimes.com/2008/12/30/nyregion/30records.html.

[5] Mike Leavitt, *Connecting the Medical Dots*, WASH. POST, Dec. 22, 2008, at A21, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/12/21/AR2008122101448.html.

[6] *See generally* Barack Obama: Technology, http://www.barackobama.com/issues/technology/ (last visited Mar. 25, 2009). *See also* Glyn Moody, *A Different VistA for the NHS?*, COMPUTERWORLDUK, Jan. 9, 2009, *available at* http://www.computerworlduk.com/community/blogs/index.cfm?entryid=1714&blogid=14.

[7] Pub. L. No. 104-191, 110 Stat. 1939 (1996).

[8] *See* Letter from Deborah Peel, MD, Founder and Chair, and Ashley Katz, MSW, Executive Director, Patient Privacy Rights, to Harry Reid, Senate Majority Leader, and Nancy Pelosi, Speaker of the House (Dec. 22, 2008), *available at*

II
NET NEUTRALITY AND BROADBAND EXPANSION

Proponents of "net neutrality" remain committed to an Internet where all content is given equal access, as opposed to a system that offers preferential treatment for certain data and application transmissions. Opponents, however, contend that the heightened sophistication and size of the type of files being exchanged, particularly video files, have resulted in increased costs to Internet Service Providers (ISPs) for providing the necessary bandwidth. In addition, opponents urge a "hands off" approach, contending that there is no need for regulation mandating net neutrality and other Internet governance issues because market forces, in conjunction with existing antitrust regulations, are already sufficient.

President Obama supports net neutrality regulation to bolster the basic premise that ISPs should be prohibited from privileging certain website content over others, and that new competitors should have the same opportunities to reach wider audiences online.[9] Indeed, Senator Dorgan, a sponsor of a previous net neutrality bill, plans to reintroduce a revised bill granting the Federal Communications Commission (FCC) authority to police net neutrality violations, given the Obama Administration's favorable stance on the issue.

Some commentators predict that net neutrality legislation will wait for the outcome of the FCC/Comcast dispute. In August 2008, the FCC ruled that Comcast had unduly interfered with users' rights to Internet content and applications of their choice when it monitored customers' usage and selectively blocked certain BitTorrent peer-to-peer Internet traffic to allegedly ease network congestion.[10] The FCC stated that it had authority to enforce a "national Internet policy" and "preserve and

---

http://www.patientprivacyrights.org/site/DocServer/L-Congress_Stimulus_v4_12.22.08.pdf?docID=4582.

[9] *See generally* Barack Obama: Technology, *supra* note 6.

[10] *See In Re Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications*, Mem. Op. and Order, No. EB-08-IH-1518 (FCC Aug. 1, 2008).

promote the open and interconnected nature of the public Internet." Since the ruling, Comcast announced plans to limit residential Internet usage and has appealed the order to the D.C. Circuit Court of Appeals, arguing that the FCC lacks authority to enforce its net neutrality principles without specific Congressional authority.[11] If the appeals court upholds the FCC's authority to enforce its net neutrality principles, then Congress and the new Administration may hold off and allow the FCC to adjudicate any violations on a case-by-case basis; if the decision is overturned, interest in net neutrality legislation may be revitalized.

However, ARRA, which provides resources for broadband and wireless broadband deployment grants, contains net neutrality language.[12] The Act obligates recipients of the federal broadband deployment grants to operate an "open access" network and adhere to the principles contained in the FCC's broadband policy statement.[13]

Indeed, the new Administration has stressed the importance of expanding broadband access to underserved rural areas and upgrading existing infrastructure to offer cutting-edge service at speeds equivalent to the top broadband nations (i.e., South Korea, Japan, Finland, the Netherlands, and France). It has been reported that the U.S. ranks fifteenth worldwide in broadband adoption and that according to an analysis by the Information Technology and Innovation Foundation (ITIF). The U.S. also trails numerous other countries in price, speed and broadband availability.[14] The Obama Administration has stated that it wants to encourage more efficient use of the wireless spectrum and advance development by, among other things, refocusing the Universal Service Fund program from one that promotes telephone communication to one that promotes affordable broadband access. Ultimately, the

---

[11] Steven Musil, *Comcast Appeals FCC Traffic-Blocking Ruling*, CNET NEWS, Sept. 4, 2008, *available at* http://news.cnet.com/8301-13578_3-10033376-38.html.

[12] Pub. L. No. 111-5, § 6001(j), 132 Stat. 115 (2009).

[13] *See In the Matter of: Appropriate Framework for Broadband Access To The Internet Over Wireline Facilities*, Docket No. FCC-05-151, 20 F.C.C.R. 14986 (Aug. 5, 2005).

[14] *See* Robert D. Atkinson, Daniel K. Correa & Julie A. Hedlund, *Explaining Int'l Broadband Leadership*, THE INFO. TECH. & INNOVATION FOUND. (May 2008), http://www.itif.org/files/ExplainingBBLeadership.pdf.

Obama Administration and Congress will have to decide in what proportion financial incentives for broadband will go toward expanding service into rural areas or upgrading existing networks to allow such high-speed services as video teleconferencing, beyond those projects for which the telecom networks have already budgeted.[15]

III
FOCUS ON INTELLECTUAL PROPERTY

In late 2008, Congress passed the Prioritizing Resources and Organization for Intellectual Property Act (PRO-IP),[16] which, among other things, enhanced the remedies for certain copyright infringement and counterfeit goods claims and created a new position within the Executive Office of the President, namely the Intellectual Property Enforcement Coordinator, or "IP Czar." President Obama will appoint the first IP Czar who will be responsible for, among other duties, reporting to Congress and the President about the effectiveness of the government's domestic and international intellectual property (IP) enforcement policies, chairing a committee to coordinate interagency anti-counterfeiting efforts, and reworking any regulatory weaknesses in IP enforcement.[17] Similarly, President Obama also pledged to name the country's first Chief Technology Officer (CTO). According to Obama's campaign website, the CTO would be charged with several duties, including directing the modernization of agency IT infrastructures, ensuring the transparency and accessibility of government records by establishing centralized electronic depositories for lobbying and campaign finance reports, and posting transcripts of agency meetings and non-emergency bills online for public comment.[18]

---

[15] Cecilia Kang, *Internet Service Speed Is Fast-Track Issue for New Administration*, WASH. POST, Jan. 13, 2009, at D4, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/01/12/AR2009011203179.html.

[16] The Prioritizing Resources and Organization for Intellectual Property Act of 2007, Pub. L. No. 110-403, 122 Stat. 4256 (2008).

[17] *See generally* Laura Sydell, *Q&A: What Will The Intellectual Property Czar Do?* NPR, Oct. 14, 2008, http://www.npr.org/templates/story/story.php?storyId=95702932

[18] *See* Jill Lawrence, *First U.S. Tech Officer Will Have Hands Full*, USA TODAY, Dec. 29, 2008, *available at* http://www.usatoday.com/tech/news/techpolicy/2008-12-29-cto_N.htm.

During the last session of Congress, many unsuccessful patent reform proposals were launched that touched on issues such as the quality of issued patents, the calculation of damages in patent litigation, the definition of willful infringement, and streamlined processes for patent reexamination. On President Obama's campaign website, patent reform is listed as one of the President's IP-related goals.[19] Among the list of proposals, he advocates increasing the United States Patent and Trademark Office's budget for patent examinations and opening up the examination process to a so-called "public peer review" to help weed out weaker patents that might otherwise spur litigation and discourage future innovation.[20]

IV
PRIVACY AND DATA SECURITY

According to a recent survey, there has been almost a fifty percent increase in reported data security breaches at businesses, government agencies and educational institutions since 2007.[21] Companies and other entities that handle sensitive consumer information are also faced with an increasingly complicated compliance task. At least forty-four states and the District of Columbia have enacted data security breach notification laws, which require, under varying standards, that companies suffering a qualifying breach of certain consumer personal information notify affected persons. Currently, there is no national data security breach notification law, but the new Administration has expressed support for passing such legislation. Several senators have expressed a desire to reintroduce data breach notification bills that died in the last Congress, yet the scope of such a new law remains uncertain. For example, would a federal law contain a "risk of harm" trigger that is, a provision that excuses notification for technical breaches of a system that do not

---

[19] *See* Barack Obama: Technology, *supra* note 6.

[20] *Id.*

[21] *See* Brian Krebs, *Data Breaches Up Almost 50 Percent, Affecting Records of 35.7 Million People*, WASH. POST, Jan. 6, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/01/05/AR2009010503046.html.

reasonably seem likely to subject affected customers to a risk of criminal activity? Another open question is to what extent, if any, a federal law would preempt existing state notification laws.

The Obama Administration has also pledged to strengthen privacy protections for the digital age, increase funding for Federal Trade Commission (FTC) enforcement efforts, and step up efforts to discourage cybercriminals by combating spyware, phishing schemes and other Internet-related privacy hazards. Federal spyware bills have died in the last three Congresses. The outlook for passage of a new comprehensive spyware bill with notice and consent provisions and a "Good Samaritan" provision that would limit remedies against anti-spyware software developers is mixed, particularly given Congress's recent cybercrime amendments.[22] The cybercrime amendments, among other things, increased the capabilities of the federal government to prosecute those behind malicious spyware, enabled identity theft victims to obtain restitution for the time and money expended in clearing up their credit, and criminalized the use of malicious spyware and keylogging software that caused computer damage.[23]

V
BEHAVIORAL ADVERTISING

Another possible privacy initiative is online behavioral advertising, an issue addressed by the FTC and the last Congress. Generally speaking, behavioral advertising is the tracking of a consumer's online activities (e.g., search engines queried and Web pages visited and content viewed) in order to deliver advertising targeted to the individual consumer's interest. In theory, consumers would view ads that appeal to their interests, thereby allowing companies to better reach their target markets. For social networking sites, behavioral advertising can serve as an additional revenue source. Still, some advocates have claimed that such advertising threatens individual privacy and have called for the user

---

[22] Identity Theft Enforcement and Restitution Act of 2008, H.R. 5938, 110th Cong. (2d Sess. 2008).

[23] *Id. See also* Brian Krebs, *New Federal Law Targets ID Theft, Cybercrime,* Wash. Post, Oct. 1, 2008, http://voices.washingtonpost.com/securityfix/2008/10/new_federal_law_targets_id_the.html

opt-out protections. In late 2007, the FTC staff issued a set of proposed principles to encourage development of self-regulation for online behavioral advertising, as well as address consumer privacy concerns over personal data collected by social networking and other websites.[24] A full report is expected sometime this year.

Behavioral advertising on the ISP level has also become an emerging issue. In 2008, NebuAd,[25] an online advertising company, began a behavioral advertising program in conjunction with several ISPs, allegedly without the consent or knowledge of the ISPs' users. The program ended when Congress began to make inquiries.[26] Subsequently, during a Senate committee hearing on behavioral targeting, many leading ISPs agreed in principle to stop the practice and only engage in behavioral targeted advertising with the affirmative consent of users.[27] While the Obama Administration has not specifically professed a position on behavioral advertising, Congress will likely monitor this issue and determine whether the industry's self-regulatory efforts offer sufficient consumer protections, or whether a data privacy bill authorizing stronger FTC regulation of the online advertising industry is required.

---

[24] *See* Press Release, Federal Trade Commission, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20. 2007), *available at* http://www.ftc.gov/opa/2007/12/principles.shtm. See The Network Advertising Initiative, *The 2008 NAI Principles: The Network Advertising Initiative Self Regulatory Code of Conduct* (2008), http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf, for the principles of a private regulatory organization of companies in the online advertising.

[25] http://www.nebuad.com/ (last visited Mar. 25, 2009).

[26] *See generally* Ellen Nakashima, *NebuAd Halts Plans For Web Tracking*, WASH. POST, Sept. 4, 2008, D2, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html.

[27] *See* Brennon Slattery, *Big Brother ISPs are Watching,* PC WORLD, Sept. 26, 2008, *available at* http://blogs.pcworld.com/staffblog/archives/007805.html. *See also* Valentine v. NebuAd, No. 08-5113 (N.D. Cal. Nov. 10, 2008) (Putative class action complaint filed against NebuAd and several ISPs, alleging, *inter alia*, claims under various federal and state computer privacy laws).

In the end, the new Administration has expressed a desire to tackle other, larger privacy issues that purportedly affect the national economy and homeland security. For example, President Obama's website lists several initiatives in this regard, including protecting the IT infrastructure from cybercriminals and coordinating a national cyber policy that works to shield federal agencies and private entities from attacks and data theft.[28] Moreover, the new Administration may look to update the federal electronic privacy, computer crime, and surveillance laws, as well as examine the growing concern over the security of electronic data and computer laptops during border searches in response to the Ninth Circuit's ruling in *United States v. Arnold.*[29] Regarding border searches of electronic devices, a bill, H.R. 239, has been introduced in the new Congress, which would, among other things, limit border searches of digital electronic devices to those under reasonable suspicion.[30]

---

[28] *See* Barack Obama: Technology, *supra* note 6.

[29] United States v. Arnold, 523 F.3d 941 (9th Cir. 2008) (holding that the Fourth Amendment does not require government agents to have reasonable suspicion before searching laptops or other digital devices at the border, including international airports). *See e.g.*, Associated Press, *Critics wary of Laptop Searches at Border,* MSNBC, Dec. 8, 2008, http://www.msnbc.msn.com/id/28113582/. *See also* Barack Obama: Technology, http://www.barackobama.com/issues/technology (last visited Mar. 16, 2008).

[30] The Securing our Borders and our Data Act of 2009, H.R. 239, 111th Cong. (2009).