AMERICAN MARKETER

Business at its best

COLUMNS

Exploring legal challenges to fulfilling the potential of mHealth

January 27, 2015

Joseph I. Rosenbaum is partner and global chair of the advertising technology and media law practice at Reed Smith

By Joseph I. Rosenbaum

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual."

- Earl Warren, 14th Chief Justice of the United States

In less than a week we will celebrate the 522nd anniversary of the date Christopher Columbus - an Italian explorer sailing under the sponsorship of the Spanish monarchy - landed in San Salvador in the Bahamas in 1492. While myths abound that Columbus set out to prove the world was round, not flat, nothing could be farther from the truth. Long before Columbus set sail, most important scientists and thinkers already believed the earth was a sphere. Pythagoras recognized the Earth as spherical in the 6th century BC and Aristotle acknowledged our planet was a sphere in 330 BC. Eratosthenes, a Greek mathematician, actually calculated the Earth's circumference at 21,420 miles in 240 BC - an underestimate of only about 10 percent.

Columbus had the latest technology - sailing ships, maps, compasses and sextants - [so] he clearly knew how to go and where he wanted to go. He knew he wouldn't fall off the edge of the Earth, but also did not underestimate the dangers of exploring unknown and uncharted seas. What he didn't know and what no one could predict, is where he would end up and what the many astounding consequences of his discovery might be. Today, we know he was not the first to discover our new world, but the voyages of Columbus marked the beginning of centuries of European exploration, conquest and colonization - voyages that changed the course of history.

The history of mobile technology has similarly taken off in one direction and then, like a ray of light through an unexpected prism, bends sharply another way. Jules Verne's fictional voyages to Earth's moon and even Buck Rogers cartoons of the 1930s correctly depicted the outlines of space craft, clothing and equipment that ultimately came into use for space exploration in the 1960s. But as science writer Isaac Asimov noted, nobody predicted the most remarkable aspect of the moon landing when it actually happened - that the whole world would be watching on live television. Similarly, advances in mobile technology may have us look back at Desert Storm, beyond the military victory, and judge it most importantly as the first war to be eye witnessed in detail by masses of civilians the world over, due to the tireless work of just one reporter accompanied by a cameraman and a little portable telecommunications disc.

Although not necessarily related to mobile technology, the medical and health care industries are not immune to unintended and unforeseen consequences. According to VentureSource (a database owned by Dow Jones), venture capital over the last 15 years has shifted interest away from cardiovascular and orthopedic investments to treatments

involving eyes, ears and age-related ailments. Venture capital funding of new and emerging technology often means the difference between a new and useful innovation reaching the public or dying on the vine, given the cost and regulatory hurdles of getting these products into the market. While it is hardly conclusive, it may well be that the hurdles and delays in obtaining regulatory approvals and the corresponding costs and difficulty in exploiting cardiovascular, spinal and orthopedic innovation in the marketplace, makes other forms of bio-medical and health related investment more attractive and more likely to bring greater and more rapid returns.

Hitting closer to home, if not right on target, less than a month ago, reports surfaced about consumers, many of whom are software engineers with diabetic family members, who had developed an open source system that "hacks" into a glucose monitoring device, enabling it to upload and transmit blood sugar data measured by the unit to the Internet - something it was not designed or enabled to do. Parents, care givers, children with elderly and infirm parents, could now monitor blood-sugar levels virtually anywhere with an Internet/Web enabled mobile device. Needless to say, it (the open source "hack") hasn't been approved by the Food and Drug Administration, nor by the manufacturer of the device. Yet, it highlights a significant development and a pattern we may well come to accept as inevitable. Consumers are taking an increasingly active role in their own health care and the information and delivery of health-related information in a form they can use.

Tech-smart consumers are tinkering - reportedly tweaking hearing aids to play music and using 3D print technology to make customized prosthetics, among other things. The Massachusetts Institute of Technology recently hosted a "hackathon," challenging engineers and students to improve medical products and find treatments and cures for common diseases. The most recent one was aimed at improving breast pumps and it certainly was not the first such event. Should we welcome expanding the reach of innovation and widening the circle of potentially lifesaving treatment or be concerned that we are increasing the risk of consumer reliance on dangerous products and services without the rigors of clinical trials, properly conducted research and study and regulatory oversight?

So, the voyages of Columbus and the myriad of historical examples of technology striking off in an unpredictable direction should serve as a useful metaphor for our discussion today about privacy and data protection in the mHealth environment. We have witnessed the rapid evolution of mobile technology. We know innovation will grow and technology will evolve. We don't, however, know in what ways or with what consequences. Our efforts may seem much like attempting to change a tire while the vehicle is still moving, but as daunting as that may seem, that is our challenge.

Mobile technology in health care

"We are dealing with a new technology, whose applications are just beginning to be perceived and whose capacity to deprive us of our privacy simply cannot be measured in terms of our existing systems or assumptions about the immutability of the technology."

- Arthur R. Miller, Harvard Law Professor, then of the University of Michigan, in 1968

If information is power, more and better health-related information can provide powerful tools in the search for preventive measures, diagnostic tools, treatment protocols and perhaps cures. We know that consumers, patients, health care providers and institutions, researchers and government health officials all benefit from better and more timely information. From those who monitor, detect and respond to societal health care issues, to those who protect society from misinformation about health care. From those who regulate the mobile spectrum, to those who are responsible for striking a balance between the risks and rewards of new and better health care solutions, from medication to equipment. Big Data may yield information about trends and patterns yet unseen, leading to new clues and potentially more rewarding avenues for research and treatment. Crowd sourcing may enable massive collaboration and information sharing among and between all of the participants in the chain of health care, education and research, sparking greater creativity, innovation and, ultimately, solutions to health care problems of today and tomorrow.

Mobile devices are no longer merely communications tools. Wirelessly we surf the Web, pay bills and transfer money, buy goods and services, entertain ourselves, read books and conduct research. The United Nations projects there will be 6.8 billion cell phone subscriptions, with a total world population of just over 7 billion. According to information compiled by Greatcall, there are currently over 97,000 mobile apps related to health and fitness, 52 percent of smartphone users used their smartphones to gather health-related information and there are over 4 million downloads of free mobile apps every day! Looking at the provider side of the equation, their data suggest that 40 percent of physicians believe mHealth technology can reduce the number of office visits and 93 percent believe that mHealth apps can actually help improve the health of their patients. Although 80% of the physicians

believe that mHealth apps can actually help improve the health of their patients. Although 80% of the physicians surveyed said they use smartphones and medical apps, only 25 percent of physicians actually use mobile technology to provide patient care. It is not clear how many physicians use mobile devices or apps to gather information, interact or do research professionally, and whether they consider these apps as direct patient care.

Our mobile devices store vast amounts of information about us and our connections and transactions, carried wirelessly through commercial, for-profit telecommunications networks, backed up and stored in commercially provided cloud computing environments and retrieved through passwords and encryption methodologies generally established and operated by commercial enterprises - some not even based in the United States. A recent article in the *Wall Street Journal* notes that the database of U.S. landline and cellphone numbers - the information repository that allows phone numbers identified with you to be portable when you switch carriers - is also the database relied upon by law enforcement and intelligence officials seeking wiretaps or conducting surveillance. Recently, an advisory panel of the Federal Communications Commission recommended moving custody and operation of that database to a subsidiary of a foreign corporation.

Social media across mobile platforms is another growing concern in the health care arena. Patients and care givers want to share information and often obtain information through social media. Studies have shown that consumers trust each other more than advertisers, sponsors and those with a commercial interest in the individual's purchase decision-making process. Yet there are no controls, and likely there can be no controls, on these peer- to- peer conversations. Decades ago, word of mouth was important locally. Today, with mobile technology, an mHealth-related conversation among consumers can potentially reach over 6 billion people with the press of a button. Since more people now use mobile devices to surf the Web, communicate and gather information, it is clear that mobile technology, coupled with social media platforms and cloud computing capabilities, is and will continue to have a transformative effect on the delivery and distribution of health care products and services, the education and experience of our health care providers and the operation of our health care institutions, not to mention our government and insurance companies involved in the health care and mHealth environment.

Mobile technology provides everyone in the web of health care with unparalleled potential benefits as well. Today, "apps" (smartphone applications) allow me to access medical records and to contact physicians and health care providers. A commercially available service ensures a physician will be on-call and available to me, not only to listen to any medical problem that arises, but to recommend and arrange treatment - all with the tap of an app. Toothache? No problem, dentists are a mobile search away. Lost or forgot your prescription medication while away from home? Easy to remedy with apps and mobile devices at your fingertips. Often, physicians can use the interactive mobile capability to request prescriptions be electronically transmitted to the nearest local pharmacy. Have a question about health - diet, nutrition, exercise, drug interactions, symptoms or ailments? Yes, there's an app for that.

With mobile technology we can obtain test results almost as quickly as our insurers, schedule appointments, exchange information with health care professionals, search for multiple sources of health-related information miles from the nearest library, and we can even measure pulse and respiratory rates, vital signs and a host of metrics. Welcome to the medical and health related benefits of wearable technology, coupled with wireless and mobile devices that can upload, download and communicate information anywhere, to anyone, in real time. Mobile applications are connected with insurance and government reimbursement systems, as well as billing and payment systems, making even the administrative aspects of the health care process more efficient and more risky.

Privacy and mHealth

"The privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy."

- Larry Ellison, CEO, Oracle, 2001

From a legal viewpoint, privacy is protected by law and regulation and enforced by the courts, not merely because the individual has a subjective expectation of privacy, but because that expectation is considered reasonable in the context of current social practices and values. As a result, it is also important to examine and understand how mobile technology is rapidly changing the individual's reasonable expectation of privacy and the concept of what is socially acceptable or reasonable to expect. Let's first look at privacy from a legal and regulatory perspective.

Territorial privacy is traditionally associated with the physical right to be left alone or undisturbed. The idea that we should not be disturbed by loud noises or environmental toxins is based on the physical requirements we seek to

impose on our surroundings. Without being invited or given permission (in a legal sense, without a warrant), no one is allowed into our space.

Another concept of privacy relates to privacy of the person or individual. The United States has constitutional guarantees and laws relating to freedom of movement and expression, restraints against unlawful searches and seizures and prohibitions against physical assault and non-physical harassment (e.g., discrimination, defamation, sexual harassment, obscenity). Unlike territorial privacy, principles of personal privacy are not constrained by physical walls, but by social and cultural norms. Legal principles have arisen to reflect society's values, and in many ways, the concept of personal privacy relates to the protection of an individual's perceived sense of dignity. Because personal privacy is highly contextual, laws and judicial pronouncements in each jurisdiction have evolved to mirror the perceived normative values of the society. These norms change over time and judging obscenity by "community standards" or legal responses to discrimination (e.g., racial, ethnic, gender) are examples of legislative and judicial application of the law and regulation to non-physical invasions of personal privacy.

Yet another category of privacy, and one we are most concerned with in our highly networked, interconnected, digital world, is also conceptually based on the idea that an individual has the right to have his or her dignity and integrity preserved and protected. Although this perception of privacy is also highly contextual, our reference points are neither physically invasive nor technically a direct assault upon one's senses or sensibilities. This particular notion of privacy relates to the collection, disclosure, distribution, and use and abuse of information about a person. We tend to assume that information about us is ours to own and to disclose publicly and communicate to those we choose - in short, to control when, where, to what extent to whom information about us is disclosed. Competing social values and the need to function in society often require individuals to make decisions to disclose otherwise personal facts and in other cases, individuals choose to disclose private information based on personal values and relationships (e.g., to a physician or pharmacist). These decisions change and evolve over time as the nature and extent of relationships change over time, whether personal, commercial or governmental.

The Internet, World Wide Web and online technology exacerbated this aspect of privacy, and mobile telecommunications technology has multiplied that concern several billion times. That said, we cannot overlook the reality that our perception of what rights we should have, when, where, to whom, and what types of information about us we feel is appropriate to disclose, continue to be evaluated and re-evaluated as innovation, technology and social media interaction increasingly embeds itself into our daily lives.

In the health care environment, individuals not only provide information or allow information to be collected, but physicians, health care institutions, pharmaceutical manufacturers and the government, create and derive information about us and segmented groups depending upon the uses and enterprise involved. While each may have a legitimate purpose in creating, obtaining or using the information, individuals often continues to assert they have or should have a continuing right and interest in controlling how, when, where, to whom and even if that information is to be used or disclosed beyond its original purpose.

That noted, individuals are often blind to the digital imprint and consequential data they create. Electronic messages, Web browsing, transactional activity, communication and location information can not only be monitored and tracked with mobile devices, but unlike wired online activity, which is not personally identifiable in most cases, mobile technology invariably involves a device that is uniquely identifiable and an account corresponding to a specific individual. People often express generalized anxiety about the consequences of inappropriate personal information disclosure: to businesses; to people they don't know; to computer hackers; to marketing and data mining; and to companies that analyze the information in order to display advertising based on the information obtained. However, in their daily lives, they often disclose information through mobile platforms virtually indiscriminately to strangers, both individual and commercial. Most people aren't actually sure that any actual harm has occurred.

Privacy legislation, regulation, and litigation are often the results of tension and a corresponding balancing act between individuals' stated wishes to have the right to control such information, their actual behavior and activity with respect to information in their possession and control and the use of information about individuals for any other purportedly "legitimate" purposes (e.g., prevention of epidemics; research).

Security and mHealth

"Discovery and invention have made it possible for the Government to obtain by means far more effective than stretching upon the rack of disclosure of what is whispered in the closet.' Through television, radium and photography, ways may soon be developed by which the Government can, without removing papers from secret

photography, ways may soon be developed by which the Government can, without removing papers from secret drawers, reproduce them in court and by which it can lay before the jury the most intimate occurrences of the home."

- Louis D. Brandeis, Associate Justice of the United States Supreme Court

Since privacy and security are not synonymous, we need to also deal with issues that relate to the protection of both the device and the information that is stored, transmitted and used in association with those devices. Speaking at a conference this past June, Mac McMillan, CEO of CynergisTek and chairman of the Privacy and Security Task Force of the Healthcare Information and Management Systems Society, noted that roughly 41 percent of users in the health care arena don't use a password to access their mobile device, 52 percent access unsecured networks with their mobile device and admit their mobile devices are on and Bluetooth enabled all the time.

Thus, with great benefit and opportunity comes great responsibility and obligation. Absent proper security, data protection and privacy controls, how can we know if information isn't being disclosed to insurers, pharmaceutical manufacturers, researchers, our employers, advertising agencies, lead-generating companies or anyone willing to pay the price for the information. We must be rightfully concerned with the security and integrity of health care information, increasingly uploaded and backed up by mobile devices to remote, cloud-based technology. The technology must also be reliable enough so that it not only doesn't fail when it is needed most, but it moves the information rapidly, completely and accurately. Health care providers and institutions often need to make decisions quickly based on the best available information using reasonable standards of care. Waiting for pages to load on mobile devices can seem like an eternity when trying to buy theatre tickets. What if someone's life or well-being depended on information being available on a mobile device?

Concerns over operational integrity and security are not new to innovative technology and addressing these concerns must be a team effort, with all the participants in the mHealth ecosystem directly involved in the protection of devices and data. In 1968, Joseph J. Wasserstein, writing in the *Harvard Business Review*, stated "no one group should bear complete responsibility for protecting the computer system. The need for controls should be instilled in the entire organization, starting with top management and extending to all personnel." That was in 1968, when personal computers, laptops, networks, interactive services, social media, mobile technology, cellphones, smartphones, cloud computing and Big Data were unimaginable, much less in our vocabulary. In 1984, an article entitled Common Sense and Computer Security appeared in the *Harvard Business Review* in which the authors state, "Today, computer security encompasses two chief elements - the physical security of the installation and the integrity of the data." It is not difficult to apply these concepts or principles to mobile health care and information. The technology and "state of the art" has changed, but not the principles. Chains are only as strong as their weakest link.

While it goes without saying that the potential for abuse or accident exists and consequently, the security, privacy, data protection, integrity, availability, utility of devices and information are paramount in any mHealth consideration. It is also important to suggest that it would pose a greater risk to health and safety of our population if we fail to encourage, incentivize or allow the implementation of mobile, wireless, portable, innovative technology. In our hospitals, by physicians and other health care professionals, by research laboratories, scientists and academics, and for consumers and patients, we must make the advantages and benefits of mHealth technology available. Treatment of an unconscious patient, accident victims, individuals requiring medical attention remotely or while traveling, are obvious examples and the use of mHealth technology is sometimes the only alternative. Safeguards are critical, with strong measures to deter, prevent, detect and remedy abuse, but the benefits of mobile health care, wirelessly available information and interactive communication can and will certainly provide benefits we cannot imagine today.

Predictions you can't hold me to; questions I can't answer

"Insanity is doing the same thing over and over again but expecting different results."

We know that mobile technology enables the speedy and facile flow of information, unfettered by wired connections or borders. If the purpose of mHealth is to promote health in every sense of the term, then mobile technology that is secure, reliable and efficient, enabling the flow of health care services and health-related information, will yield unimaginable benefits. While we may not be able to predict the future, nor can we be sure of the consequences of our efforts or the direction the technology may follow, here are a few thoughts, predictions and suggestions to consider:

Let's recognize that digital and mobile technology have changed the environment and landscape upon

which our laws and regulations arose. While that does not mean throwing the baby out with the bath water, it does mean we cannot remain rooted in the past without appreciating the need to restructure our legal and regulatory approach to adapt to the present and prepare for the future. Are separate mHealth regulations, guidelines and enforcement proceedings emanating from the FDA, the FTC and the FCC consistent with what society and the public need in order to maximize protection, minimize abuse and optimize the cost-effective delivery of safe, effective health care in the United States? Consider restructuring regulatory oversight by integrating and networking the approach to regulation by FCC, FDA and FTC. Patients, who are also consumers, don't use mobile technology, social media platforms and cloud environments in neat categories, silos or pigeon holes - why should our regulatory framework? Can we implement meaningful and effective mHealth protections in a networked, digitally connected mobile world if we can't approach regulation the same way the ecosystem is structured? A revolutionary thought - cooperate, collaborate and create together formally, as a mandate. Institutionalize it, encourage it, believe in it. If existing legislation doesn't allow, ask for it no, press for it. If it's never been done, do it anyway - Columbus was not deterred by others too afraid to pursue the same vision.

Let's recognize the distinction that consumers, patients, health care organizations, researchers and academics have recognized for decades and apply it to mHealth technologies: the difference between "privacy" and "data protection" is not semantic or esoteric. While personally identifiable information and certain activities and transactions may truly be private, if we continue to blur the distinctions and act as if privacy and data protection are and mean the same thing, we will never align our legal or regulatory frameworks, or our systems of privacy and data protection, with what consumers, patients and health care providers have known for years. In the exchange of value, real or perceived by the consumer, the term "privacy" has become synonymous with the right to exploit the value of information about that individual, her or his relationships, activities, behavior and preferences, whether or not personally identifiable and whether or not sensitive or confidential. The law needs to catch up. Not all data or information is private, but data about, derived from, created by or associated with an individual, even when aggregated and unidentifiable, has a value and should be subject to controls - in some cases selected or approved by the consumer/patient.

Consider giving consumers and patients, in conjunction with their health care providers, greater control over how, when and for what, they will use mHealth technology and mobile platforms. Provide greater incentives for venture capital to invest in innovation that is more readily exploitable with fewer regulatory obstacles and more return on investment. Neither control nor commercial incentive should imply disregard of safeguards - but if we seek to prevent patients and physicians from having the primary right to decide the right health care path for them, if we stifle the adoption of new technology by over-regulation, if we establish too many obstacles to innovation in the mHealth arena or we fail to enable commercial enterprise to subsidize innovation in mHealth technology, either technology and innovation will go elsewhere or we will find an army of "innocent" citizens facing civil lawsuits or charged with criminal conduct for simply trying to obtain better health care. This will not be easy or simple, but I believe it can and will work.

Do not assume that implementing mHealth and telemedicine technology will be reduce the costs to the public associated with health care. By making health care available wirelessly (and even reducing the per unit cost of a particular event) the overall cost of health care may well increase as the volume and scale of delivery increases, and enterprises must include the cost of increased security and protection in the mHealth environment. The very convenience and availability of mHealth technology and corresponding information and care means we must be vigilant to ensure those systems continue to provide high quality, safe and secure cost-effective access to those who need it most. Perhaps we should include the implementation of robust privacy controls and security protections, as well as reduced cost of implementation, as a primary goal of the use of mobile technology and innovation - embedding those goals in the legislative and regulatory framework, in commercial incentives for industry and institutions, and in the interactions between patient and health care provider.

Consumers, patients, physicians, health care institutions and providers will increasingly tinker with any mHealth innovation and technology, devising mechanisms to accommodate their own needs in potentially unexpected ways. While it is clear these could pose great risk, they also may provide or lead to great benefit. Is there no way to expedite the review and evaluation of innovative mHealth devices and technologies? Striking a balance will be fundamental to any new policy directives undertaken by the government. In the same vein, consider how the use of mobile technology may stimulate collaborative research, information sharing and allow the wisdom of the "crowd" to help solve difficult challenges of mHealth. Mobile platforms will enable health care providers and institutions, as well as patients, to more effectively collaborate and coordinate, facilitating both care

and research. Rather than think of such collaborative and crowd-sourcing solutions as fraught with risk, think of them as Big Data on steroids. They will need to be monitored, but the results may be simply astounding. Crowd sourcing may provide innovative solutions to health care problems, but may lead to greater risk - with unproven and often untested remedies embraced by millions of Twitter followers or Facebook friends. Can Big Data and volume compensate for the lack of time in testing or clinical trials and evaluation? Probably not entirely, but since we likely will not make this problem go away, let's focus on the search for solutions rather than the punishment of the innocent.

Availability of mHealth information through mobile and online platforms will require more control to ensure integrity, reliability and security. Conversations about health care enabled by mHealth technology will make the need for carefully crafted oversight to avoid deception and misleading claims and information becoming accepted or mainstream simply because mobile platforms enable them to go viral. The challenge of meaningful, understandable and effective disclosures and disclaimers, informed consent and the enabling of true consumer choice in an mHealth world in which conversations can often be uncontrolled will be daunting. But appreciate that these controls cannot, should not and will not look the same as they did in the monologue world of print, radio and television communications or even as they did in the two-way communications of telegraphs and landline based telephones.

Telemedicine and mHealth technology will provide capability for greater customization of health care, but will also reduce "personal" health care, with fewer office visits, remote diagnostics and the increasing capabilities spawned by mobile technology to distribute and deliver health care remotely. This poses a greater risk to privacy and security, given the need to collect, interpret, store, process and transmit information wirelessly, in cloud environments. Indeed, everything from pacemakers and insulin pumps to diagnostic and monitoring devices, will offer malicious hackers opportunistic points of entry through mobile and interconnected networks. If one assumes that a chain is only as strong as its weakest link, how can we implement mHealth technologies in a digitally interconnected, networked environment, while protecting the privacy and security of information across mobile networks, platforms and devices?

Do not underestimate the potential breadth and scope of mHealth issues and the technology driving them. MHealth is not limited to wireless or broadband spectrum carried over telecommunications cellphone or Wi-Fi networks. Near Field Communication (NFC), Radio Frequency Identification (RFID) and Bluetooth technology, SMS (text) and similar instant messaging and content sharing technology must be considered as part of the mHealth ecosystem. Similarly, content shared and transmitted by, among and to consumers and patients is no longer limited to text or oral communication. Photographs, X-rays, scan results and combined audio-visual content is now part of the "data" that require consideration. If a picture is worth a thousand words, should photographs be used to provide remote diagnostics - are they secure?

Think out of the box. The implementation of innovative mobile technology is not unique to mHealth and other industries have and continue to grapple with similar issues. Are delivery logistics that conceptually different between Federal Express [FedEx] and Pizza Hut? Financial institutions have many of the same issues. If everyone in the chain of mHealth development and delivery lives in a real world of social media, mobile devices and cloud computing, should the legal and regulatory frameworks that protect our privacy and security in an mHealth environment live in silos?

Morse Code - Telegraphing the answer

As we close this hopefully thought provoking session, let me end as we began, taking you back almost 200 years to the workings of the man that many consider to be the godparent of modern telecommunications, Samuel F.B. Morse.

Frustrated by slow mail service in the early 1830s and learning by mail of the death of his wife too late for him to attend her funeral, Morse began to develop the telegraph. He was able to demonstrate that electrical pulses could be induced that could activate an electromagnet far away. Having demonstrated the ability to do so, he devoted a decade trying to concoct an elaborate instrument to make these signals more useful and practical - inventing a device that could receive these signals and print the individual letters and numbers on a moving piece of paper. In theory, not much different from today's digital printers. In fact, it worked - although agonizingly slowly.

What Morse had never considered, now the stuff of legend, was the existence of another computer that uses a self-generated electrical supply with less drain than a 20-watt bulb, having enormous memory capacity, which is largely self-correcting, comprising over a hundred billion processing elements all linked by a hundred trillion connectors.

The human brain of the telegraph operator who, receiving the unexpected auditory stimulus, quickly learned to bypass Morse's cumbersome printer and "read" characters by ear, hearing them as dots and dashes from the sound of the machinery. Overnight, and quite to the surprise of Morse, the speed and accuracy of telegraphic messages improved a hundred-fold and made the telegraph commercially viable and an effective communication tool. The rest, as they say, has been history.

As with Columbus before him, there was no question in Morse's mind whether he could reach his goal (in Morse' case, sending electromagnetic signals) or even whether he could figure out how to accomplish this revolutionary feat. But just like Columbus, in the end Morse had no idea what the discovery which revolutionized communication would look like - or in this case, sound like.

I have no doubt similar events and consequences will bedevil us as mHealth technology and innovation continue to leap forward and as the government, technology and communications industries, patients and consumers, health care professionals and institutions increasingly adopt and use mobile platforms to improve the cost-effective delivery of high quality health care in the United States.

To act or not to act. Is that really the question?

In conclusion, let me acknowledge there are those who would argue that changing perceptions, norms and social context demand we defer and delay any legislation or regulation that attempts to deal with such a moving target. After all, claims that legislation or regulation is and will be obsolete on the day signed into law or enacted have a certain popular appeal. Privacy and security and the protection of information and the consumer, especially with respect to health care, have always been difficult and challenging, made more so by rapidly evolving and changing technology.

There are others who will find it equally unacceptable to ignore fundamental changes and permit abuses to continue while the "dust settles." In fact, one might ask if the dust will ever really settle. If we accept the notion that many of our ideas about privacy and security stem from personal experiences and perceptions, surrounded by the normative values of the society we live in, it is likely the law may never catch up because the problem is not static. While the dynamically evolving ecosystem must be taken into account, that should not preclude legislation to establish necessary and appropriate standards, regulation to prevent abuse and harm or enforcement to deter and address abusive behavior, unauthorized activity and illegal conduct.

The law is deeply rooted in precedent and the past. The law looks backward in order to adjudicate the present and the present is changing faster than ever before. That does not mean we should not act. It simply means we must be judicious and measured in our actions, remaining flexible more than ever to adapt quickly as the future unpredictably unfolds before us. The people and the organizations represented in this workshop clearly will have the know-how and will understand where we need to go, but we must be careful to appreciate we might not always be able to foresee the consequences or the outcome. That is our biggest challenge in mHealth today.

In 1959, in a speech in Indianapolis, IN, John F. Kennedy, who would become president of the United States, stated, "The Chinese use two brush strokes to write the word 'crisis.' One brush stroke stands for danger; the other for opportunity."

In the world of mHealth, we will continually be faced by enormous opportunities disguised as unsolvable challenges and obstacles.

This paper was initially presented on Oct. 7, 2014 in Washington as part of the mHealth and the Law Workshop convened by the American Association for the Advancement of Science, supported by a grant from the Robert Wood Johnson Foundation.

Joseph I. Rosenbaum is partner and global chair of the advertising technology and media law practice at Reed Smith, a New York-based law firm. Reach him at jrosenbaum@reedsmith.com.