JOURNAL OF OBJECT TECHNOLOGY

Online at http://www.jot.fm. Published by ETH Zurich, Chair of Software Engineering ©JOT, 2003

Vol. 2, No. 5, September-October 2003

A Snapshot of the Trends of the Internet Era: United States 2003

Won Kim, Cyber Database Solutions, Austin, Texas

1 INTRODUCTION

It has been a decade since the introduction of the World Wide Web. The first ten years of the Internet Era that the World Wide Web opened up has brought out human creativity, greed, and naiveté; has brought about major changes in commerce, governance, and human interactions; and has created several major headaches and risks for humans and the society. During the hay days of the dot-coms in the late 1990s and early 2000s, many people tended to believe that the Internet would create a virtual "parallel universe (or society)" in which "all rules that govern the 'offline' society will give way to totally new rules or no rules at all", and that the Internet would somehow be a "frictionless" engine that will drive indefinite and infinite wealth-creation. However, after the dot-com bubble burst in 2001 and 2002, such "irrational exuberance" gave way to sober economic, social, cultural, and legal realities.

I have been monitoring several aspects of the Internet with a keen interest during the past 3-4 years. In particular, I have been interested in trends in the uses (application areas) of the Internet, in both the positive and negative impacts of the Internet on humans and the society, in how the negative impacts of the Internet can and will be solved, and in the development of both the software and communications technologies that support the Internet and its applications. In an earlier article [Kim 01], I gave a snapshot of the trends of the Internet Era as seen in 2001. In this follow-up article, I will give a snapshot of the trends in 2003 in the United States. I believe there are many similarities in other Internet-active countries around the world.

In the earlier article, I classified the impacts of the Internet on humans and the society into three categories, borrowing from Sergio Leone's 1967 classic "spaghetti Western" movie titled "The Good, The Bad, and The Ugly". In the article, I defined "the good" as the positive impacts of the Internet, and "the bad" as the negative impacts of the Internet. I defined "the ugly" as the kinds of impact that come about in any type of revolution and that are settled by the passage of time, through maturing of the Internet users, and which cannot be solved by any reasonable and enforceable laws and international agreements. I threw into the "good" such things as the augmentation of the

Cite this column as follows: Won Kim: "A Snapshot of the Trends of the Internet Era: United States 2003", in *Journal of Object Technology*, vol. 2, no. 5, September-October 2003, pp.57-66. http://www.jot.fm/issues/issue_2003_09/column5

economy with an Internet-based economy, the advent of many new types of businesses using the Internet, cost savings and convenience to the consumers, the convenience and cost savings of electronic governance, the potential spread of democracy, possibilities of enhanced medical treatments via remote diagnostics and availability of medical information online, electronic distance learning to augment in-class learning and education, etc. I threw into the “bad” such things as new types of crimes that make use of the Internet (such as payment frauds, piracy of intellectual properties such as music, software, games, movies, even personal identities), conflicts between online businesses and offline businesses involving the ‘right to do business” (such as selling wines and cars online), conflicts on the levying of sales tax on things sold on the Internet, etc. I held the view then that to address the negative impacts of the Internet will require a combination of advances in technologies, new laws (and enforcement) (within a country), and international agreements (for those issues that cross a country’s border). I threw into the “ugly” such things as domain-name squatting, spam, transmission of computer viruses, the social malaise that existed as a result of the apparent “new paradigm” for wealth creation involving dot-coms, digital divide, etc.

Before I describe the trends that have emerged during the past few years, I need to make one important qualifier to my definition of the “ugly”. Certainly, some of the “ugly” things, such as the social malaise brought about by the rise and fall of the dot-coms, cannot and should not be governed by laws and international agreements. However, as the level and scope of irritation on people and the economic impact of such things as spam, domain name squatting, and dissemination of computer viruses have far exceeded what can reasonably be tolerated, there are now definite trends to combat these through new technologies, legislation and international agreements. In other words, things that belong to the “ugly” when there are no laws against them and the level of economic damage is low can be moved to the “bad”.

Now I will describe the recently emerging trends in all three categories of the impacts of the Internet on humans and the society.

2 THE GOOD

First, let us look at the “good”. The things that I included in this category still stand. Despite the bursting of the dot-com bubble, many Internet-based businesses have survived and established themselves firmly. High-visibility examples include eBay, Yahoo, Google, Overture (recently acquired by Yahoo), Amazon, America Online (despite its recent troubles), EarthLink, Priceline, Hotels, Expedia, Travelocity, Monster, CareerBuilder, E-Trade, AmeriTrade, Ditech, LendingTree, etc. The Web and the Internet are what made these new businesses possible. These businesses did not exist until the Web came into being. In fact, it is generally estimated that there has been a 30% increase in electronic commerce compared to a year ago. Many corporations now use intranet portals to communicate with employees and process employee-related issues (e.g., benefits). Many corporations use Internet portals to communicate with and provide services to customers and business partners (suppliers, vendors, etc.), including technical consultations on the use and troubleshooting of products, selling products and services, and invoicing and payments. The government, too, has made available most forms and documents available on the Web for the public to download, fill out and submit online. It is clear that these trends will continue.

During the months leading up to the US-led war on Iraq, many massive demonstrations were organized around the world against the war. The organizers used emails, websites, bulletin board and chat rooms to communicate among themselves, recruit volunteers and donations, inform (and misinform) the public, etc. [Lee 03] This was a clear demonstration of the power of the Internet for rallying the public to a political cause. This also showed that, if properly used, the Internet could indeed help to spread democracy in countries where democracy does not flourish but where the Internet is or will be in wide use. However, the Internet can also be used to amplify the voice of a vocal minority who may or may not have the wisest or right views and, when coupled with a political bias in the news media, have it dominate the "silent" or "less Internet-savvy" majority or those with the wiser or right views. The potential amplification of a certain view can have serious consequences in many areas, including politics (elections, setting of the political agenda, etc.), public policy-making, foreign relations, allocation of government funding and resources, etc. It is hoped that governments, news media, and people all learn to take the Internet-based input as merely one form of input in making the best-informed decisions. Until then, this aspect of the impact of the use of the Internet will belong to the "ugly" category.

3 THE UGLY

During the dot-com frenzy, some "investors" forked over millions of dollars to would-be entrepreneurs on the "strength" of concepts scrawled on the back of napkins over drinks, rather than traditional formal business plans. Investors directed the executives of the start-up companies thus created to spend and spend, without worrying about generating revenues or profits, just so that they can generate the largest number of non-paying website visitors. Many companies spent lavishly on parties and fully stocked kitchens for employees, and offered stock options, disproportionately large salaries and bonuses, signing bonuses and expensive automobiles, etc. to both the executives and key employees. Start-ups with no product and no customer openly talked about their estimated stock-market capitalization being in the hundreds of million dollars. Even many office-building owners in Northern California demanded and received stock options from high-tech start-up tenants on top of substantial rents. Some company with a few million dollars in revenue acquired another company with a few million dollars in revenue, and the industry financial analysts put the market capitalization of the combined company in the billion-dollar range. The "business" model of some company was to give free PCs in exchange for a promise to watch ads that would pop up on the PC screen. Some company disabled a PC to limit its functions to that of an Internet appliance (for Web access), and sold it below the cost of the PC. There were other companies like this that lost money on every sale they made, such as certain online companies that sold and delivered pet food, groceries, gourmet food, etc. Some companies got into the business of selling cars and wines online, apparently not knowing that many states had laws that prohibited sales of cars and wines by anyone without physical stores and licenses. The absence of a revenue/profit model of doing business dumbfounded more traditional businessmen and business school professors, and the stories of the births of twenty-something near-instant millionaire forced traditionally well-to-do professionals such as the medical doctors and lawyers into depression over their relative "poverty".

When the dot-com bubble burst, most of the "investors" lost most of the money they gave the start-ups; dot-coms fled the lavishly furnished offices they had occupied with most of the furniture unmoved, and liquidated the offline businesses they had acquired. With mass layoffs, many restaurants and bars that served as hangouts for employees of those start-ups have closed or are not crowded any more; air planes have many more empty seats; hotels have many more empty rooms, and even highways in high-tech cities are now considerably less congested during normal rush hours. The sudden shutoff of the free and wild spending by the dot-coms, along with the corporate bookkeeping scandals that first become public due to the Enron accounting scandal, contributed to the onset of the economic downturn in the US and subsequently worldwide. As there is a silver lining to a cloud, the dot-com bust has had one positive impact on humans, in that the social malaise of the blind greed, envy, misguided notions about wealth creation that bordered on outright fraud have considerably subsided, and people and businesses have regained a sense of proportions and of traditional value.

However, the dot-com frenzy still has some lingering effects, both good and bad. Not all dot-coms have disappeared. Many have been able to survive the massive shakeout and are now prospering. Many other dot-coms were able to take the cash after early IPO (initial public offering) of their stock in NASDAQ, and some have been using the cash to survive while attempting to identify and implement more traditional business strategies. Whether they will be successful is unclear.

One serious lingering effect of the dot-com frenzy is the mindset of the Internet users that was inspired during the early days of the Web. The mindset is that the virtual society formed via the Internet should be guided by rules that are very different from the "tired and abominable" rules that govern the offline society. The new rules to govern the virtual society are to be based on such notions as "governments should not regulate the Internet, so that the Internet should always be 'free'", "electronic commerce, that is, all commercial transactions done on the Internet, should be free of taxation", "all contents on the Internet should be freely accessible to everyone", and "everyone should be free to express his/her opinions and do many things on the Internet without fear of being traced back". In my view, these notions have led to the wanton exchange and publishing of copyrighted commercial properties, such as music, games, movies, books, software, and even host keys to activate commercial software, with utter disregard for intellectual property rights, monetary damages inflicted on authors, corporations, and even governments. It is my opinion, too, that these notions led hackers to regard hacking and dissemination of computer viruses as "innocent, fun, intellectual exercises or games", with no consideration of the monetary damages to corporations, governments, and individuals. These have also partially led spammers to launch massive volumes of spam without feeling the least bit guilty of the time they are wasting for hundreds of millions of people and costing ISPs (Internet service providers) a lot of money to store and transmit those mails.

There are certain things that currently belong to the “ugly” category but are likely to move to the “bad” category, as it is likely, given the nature of these things, that laws will be used to stop or regulate them. These include unsavory websites that publish crime-aiding information (e.g., how to make bombs at home), that publish third party’s proprietary information (e.g., host keys for activating commercial software, credit card data), that recruit suicide partners, etc. These also include websites that dispense incomplete medical advice (which may be used by the unsuspecting public for potentially erroneous self-diagnosis), etc. Despite the dot-com bust, there are still many websites that are of such nature.

4 THE BAD

There is one “bad” thing that has been moved from the “ugly” category and has largely been solved. It is the problem of domain-name squatting. During the hay day of dot-coms, many individuals registered Internet domain names, such as “business2000”, “ExxonMobil”, “whitehouse.com”, etc., for the sole purpose of selling them to the highest bidders. One particular individual is said to have registered 12,000 domain names. Certain domain names have been sold for hundreds of thousands of dollars or even millions of dollars. ICANN (the Internet Corporation for Assigned Names and Numbers) stepped in and offered to arbitrate the domain-name disputes [Stell02]. About 3,700 domain name disputes have now been arbitrated and the generally prevailing rule (about 80% of the disputes arbitrated) is that the business entity that had first used the name in business prevails over the individual or business entity that later uses the name for Internet domain. It is interesting to observe that this rule has been established since in over half of the disputes, corporations were able to put up the will and a relatively small amount of money for arbitration, while the individuals squatting on the domain names did not have the will or the money to even show up for arbitration, forfeiting the domain names.

Currently, there is a serious debate on taxation on e-commerce. The issue is whether to impose a sales tax on items purchased online, and how to distribute the tax money collected by the merchants. On one side, the US federal government and major online merchants such as eBay and Amazon are opposed to taxing e-commerce. On the other side, 31 states and major retailers such as Wal Mart and Sears Roebuck are for it. Under the current law, businesses must collect sales tax when they sell items in states in which they have physical stores. This automatically forces all major retailers with stores in every major city in the US to collect sales tax, whereas it exempts “pure” online merchants from sales tax (except where they have warehouses) [Tedes03]. Further, major retailers have the know-how to collect and distribute sales tax. This is why major retailers are for taxation, while online merchants are against it. There are a few key reasons for the opposition. One is that although it may seem exceedingly simple, computing and distributing sales tax is very difficult, since there are some 7,500 state and municipal tax jurisdictions in the US, and many of these have different rules on tax rate, items exempt from tax, etc. Another is that many businesses actually already collect sales tax on items sold online, and additional tax collected under a mandatory sales-tax law will not be substantial. Another is that online sales are similar in nature to catalog-based sales, and the same taxation rules should apply. In any event, given the serious financial difficulties that many states face today, and given the "fairness" issue between online merchants and offline merchants, I believe that a simple flat tax rule will eventually be legislated and applied to both types of merchants and tax money will be distributed in some simple way to all tax jurisdictions. Simply put, there is nothing special about online sales: a sale is a sale, and if there is to be sales tax on offline sales, there should be sales tax on online sales.

Today the most serious item in the "bad" category is spam. Currently, it is estimated that 50% of the emails that an average email user receives daily are spam, and the rate may reach 70% by next year. Spam includes those being sent by "professional" spammers (often called master spammers) and by legitimate corporations. Master spammers acquire email addresses by using software that "harvests" email addresses on the Internet, and each send millions or even tens of millions of emails a day. They use software to identify unguarded proxy computers and relay computers on the Internet for use in sending emails and avoid being traced. They peddle products and services ranging from generic Viagra, "penis enlargement", debt consolidation, and ink-jet cartridges to porno-site membership and "marriage brokering with beautiful Russian women". Estimated 150-200 master spammers in the US are responsible for such everyday repeated irritations [Hanse03a] [Hanse03b]. They receive fees from advertisers based on positive replies received; an average master spammer is said to receive from a thousand to tens of thousands of dollars a week. It is interesting that the life of a master spammer is not an easy one, since he has to constantly stay one step ahead of the ISPs that try to filter spam, and he receives thousands of well-deserved damning and abusive emails in return. Some of them actually get frustrated and demoralized and leave the "profession" after a brief stint [Kosse03].

The US government is currently considering legislation to combat spam, including the CAN SPAM Act [Hanse03a]. Lawmakers face a number of difficulties in efforts to legislate spam. One is the promotional emails from "legitimate" corporations to their customers or those that obtain email addresses who had explicitly agreed to receive emails when they signed up for magazine subscriptions, professional society memberships, etc. Another is the legal difficulty of defining "fraudulent emails" and also penalizing violators, although about 4% of spam today are said to be "fraudulent". For example, under the current law, a misleading "subject" of an email, such as "enlarge your penis", does not constitute fraud. Further, it is very difficult to identify master spammers by tracing their emails and computers from which they emanate. However, because just about everyone is furious about the number of spam they are currently subjected to on a daily basis, the US government is sure to enact new laws and start enforcing them in the next few years.

Currently, there are many technological solutions to detect and filter spam [Schwa03][Jesda03][Maney03]. These include signature comparison (by Brightmail and Cloudmark), collaborative (voting) decision (by Cloudmark), corporate gateways (by CipherTrust, NetIQ, etc.), rule-based term search (by McAfee, SpamAssassin, Elron Software, etc.), Bayesian learning (by Microsoft, Spammunition), white list (list of pre-approved senders) (by Habeas, AOL), vaccination (email address hiding) (by Matterform, Sneakermail), and challenge-response (sender needs to answer a question to get through) (by EarthLink). The current technology gives a filtration rate (successful detection of spam) of 70 to 95%, and a false positive rate (identifying valid emails as spam) of 0.001 to 0.1% [Schwa03]. A new trend is to make it costly for the senders suspected of being spammers. One idea is to have the sender pay a tiny amount of money to send each email. For ordinary users, the amount is insignificant; however, for someone who sends millions of emails, it can add up to thousands of dollars and eat away whatever fees they collect from advertisers. Another idea is to return the email to the sender suspected of being a spammer and have the sender's email system solve some compute-intensive problem and then allow the email to reach the recipients. This is to add a processing overhead to spammers; however, it is not clear this scheme will work, since spammers use other people's computers. One key element in the eventual technological solution is the ability to trace and identify the senders of emails, however distasteful this may seem to privacy advocates.

The US government has started prosecuting those responsible for creating and disseminating computer viruses and those involved in online piracy of intellectual properties. Recently, one of those who created and disseminated the Melissa virus has been sentenced to a 20-month prison term [AP 2002]. The fact that the Philippines has no law to prosecute virus creators and disseminators points to the need for an international agreement. The Filipino man who created the I Love You virus and spread it worldwide, instead of being prosecuted, has become something of a national hero, for showing that "a Filipino can do 'it' (achieve a level of high-tech 'sophistication' and world 'renown', I suppose)". The technological solution needed to help stop the dissemination of viruses and denial of service attacks is the ability to trace the senders of the viruses. Coupled with the need to trace the senders of spam, I believe sooner or later sender traceability will be added to communications on the Internet.

Also, those that belonged to an online piracy club named DrinkorDie have been arrested and one of them has been sentenced to a 46-month prison term [Lee 02b]. There are some 30 online piracy groups involving about 5,000 members, who steal and distribute, primarily as hacking challenge, software, games, movies, and music. These include FairLight, Razor1911, POPZ, FTF, Immortal DVD, etc. A club typically consists of two groups of members. One hacks into vendors of intellectual properties, and downloads files. Another uploads the stolen files to hundreds of websites for downloading by the "public" for free. It is interesting to note that those who belong to these clubs are not motivated by money, since, as one of those arrested stated, “they can get any software, music, movies, etc. for free, so they do not need money”.

The Recording Industry Association of America (RIAA) took the initiative by going after music file-sharing websites, first Napster, then KaZaA, Aimster, Glokster, AudioGalaxy, Morpheus, etc. At one point, Napster enjoyed the distinction of the website with the highest membership on the Internet. The court easily ruled that music file-sharing websites that allowed tens of millions of people to exchange free of charge music files loaded from commercial CDs violated copyright laws on the music. As is almost always the case, the one with the deep pocket can drive into submission one with much less financial wherewithal, and Napster went out of “business”, if one can call it that. The RIAA is now going after KaZaA, which tried to avoid the reach of the US laws on copyrights by having its computer servers located in Denmark, its distributors located in Vanuatu Island, “business” managed in Australia, its software source code kept in Estonia, its programmers “working” in the Netherlands, and its millions of users in the US [Harmo02]. The RIAA has now started what appears to be the final step in their pursuit of copyright violators; they are going after a small sample of “end users” of the file-sharing programs, that is, high school or college kids. Using the outrageous but legal “up to $150,000 per song illegally downloaded”, the RIAA is trying to scare the end users into giving up their practice of downloading music files without paying [Graha03]. Apple Computers has taken a different approach by starting its I-Tune Music Store. I-Tune charges 99 cents per song downloaded [Strau03]. This appears to be a compromise of a sort by charging a relatively modest fee to discourage the scofflaws from breaking the law. It is not realistic to expect “illegal” file sharing to stop completely, just as it is not realistic to expect people not to photocopy copyrighted books that prohibit photocopying or to expect people who rent videos not to pass them to friends before returning them to the store. However, it is clear that the combination of the legal actions the RIAA has aggressively taken and the legitimate business model that Apple Computers has introduced will go a long way to curbing the illegal and unpaid sharing of music on a massive scale.

Various technological solutions to the problem of guarding intellectual property rights on digital contents are now available, although there is still a lot of room for improvement in terms of flexibility, ease of use or application, and air-tightness. These include watermarking (hiding extraneous codes in digital contents), traitor tracing (identifying people who distribute digital contents without authorization), special encoded tracks on CDs and DVDs, content scrambling of CDs and DVDs, etc. One particular challenge is to allow a person who pays for digital contents to transfer them to a limited number of “friends”, including various devices for personal use (a laptop, a PDA, etc.).

5 CONCLUDING REMARKS

Today, nearing the tenth anniversary of the birth of the World Wide Web, the Internet and the Web have been firmly incorporated into people's daily lives in the US and all other industrialized nations of the world. Despite the massive dot-com failures 2-3 years ago, electronic commerce is definitely on the rise, and electronic governance and adoption of the Internet and the Web in business interactions are firmly established. However, new types of crimes, such as e-commerce payment frauds, spam, computer viruses, and hacking, and thefts of digital intellectual rights are also definitely on the rise. Solutions to these problems will require several elements: advances in technologies, revised and new laws (and vigorous enforcement of the laws), international agreements, education of the public, and new business models. In the US law enforcement agencies and the courts have started applying existing laws governing fraud and unauthorized use of others' properties to prosecute the perpetrators. Congress has been working to draft and pass laws to bring order into the current situations. Various technology companies have also offered technological solutions to spam, viruses, guarding digital contents, etc. At the federal and state governments, debates are under way regarding the levying of sales tax on online commercial transactions. In the foreseeable future, there will be movements towards international agreements to deal with a range of issues including online crimes, digital rights, privacy, spam, viruses, and e-commerce taxation. The Internet Era is upon us, and efforts are needed to address the "bad" aspects and to make the "ugly" bearable, as well as to make the most of the "good" to help humans and the society.

REFERENCES

[AP 02] Associated Press, "Virus Maker Sentenced", *The New York Times*, May 1, 2002.

[Graha03] Jefferson Graham, "RIAA Goes After the Little Guys", *USA Today*, June 26, 2003.

[Harmo02] Amy Harmon, "Music Industry in Global Fight on Web Copies", *The New York Time*s, October 7, 2002.

[Hanse03a] Saul Hansell, "Finding Solutions to Secret World of Spam", *The New York Times*, May 5, 2003.

[Hanse03b] Saul Hansell, "Diverging Estimates of the Costs of Spam", *The New York Times*, July 28, 2003.

[Jesda03] Anick Jesdanun, "A Silver Bullet for Spam That Might Backfire", *Austin American-Statesman*, July 7, 2003.

[Kim 01] Won Kim, “Internet Technology: The Next Phase”, *Journal of Object-Oriented Programming*, January 2001.

[Kosse03] Jeffrey Kosseff, “Confessions of a Spammer”, *Austin American-Statesman*, July 7, 2003

[Lee 02a] Jennifer Lee, “Spam: An Escalating Attack of the Clones”, *The New York Times*, June 27, 2002

[Lee 02b] Jennifer Lee, “Pirates of the Web”, *The New York Times*, July 11, 2002.

[Lee 03] Jennifer Lee, “How the Protesters Mobilized”, *The New York Times*, February 23, 2003.

[Maney03] Kevin Maney, “Gates, Microsoft Look for Ways to Zap Spam”, *USA Today*, June26, 2003.

[Schwa03] Evan Schwartz, “Spam Wars”, *MIT Technology Review*, July/August 2003.

[Stell02] Susan Stellin, “In Fights Over .Com Names, Trademark Owners Usually Win”, *The New York Times*, June 24, 2002.

[Strau03] Neil Strauss, “Apple Finds the Future for Online Music Sales”, *The New York Times*, May 29, 2003.

[Tedes03] Bob Tedeschi. “The Battle Over Online Sales Tax Turns Acrimonious”, *The New York Times*, February 17, 2003.

About the author

Won Kim is President and CEO of Cyber Database Solutions (http://www.cyberdb.com) and MaxScan (http://www.maxscan.com) in Austin, Texas, USA. He is also Dean of Ewha Institute of Science and Technology, Ewha Women's University, Seoul. Korea. He is Editor-in-Chief of ACM Transactions on Internet Technology (http://www.acm.org/toit), and Chair of ACM Special Interest Group on Knowledge Discovery and Data Mining (http://www.acm.org/sigkdd). He is the recipient of the ACM 2001 Distinguished Service Award.