http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 4 (2): 151-157, 2005
ISSN 1812-5638

Intellectual Property Strategies in Security and Privacy

Dennis Fernandez, Laurie de Leon and David Kemeny
Fernandez and Associates, LLP, 0147 El Camino Real Suite 201, Menlo Park, CA 94025, USA

INTRODUCTION

Current technological advances ranging from biotech and nanotechnology to electronics and software can be used to both protect and jeopardize the security and privacy of individuals. This study highlights some Intellectual Property (IP) strategies to successfully navigate the competitive landscape of these technical industries. Because IP rights are essential in today's technology-driven age[1]. This study presents a brief overview of intellectual property rights and the various areas in the latest security and privacy technology fields to which IP rights may be applicable. The value of an IP portfolio is of interest to startups and their investors, whereas licensing agreements are of interest to manufacturers and customers.

Intellectual property overview: Some find the concept of intellectual property hard to grasp, often because it's hard to determine the monetary worth of ideas. One simple example of the value of intellectual property is the common occurrence of expensive and high-stakes infringement lawsuits. One of the costliest examples is the decades long case of Eastman Kodak vs. Polaroid, which resulted in the destruction of Kodak's instant photography business, as well as more than $3 billion dollars in infringement damages, compensation and legal fees and research and manufacturing costs[2]. Even lawsuits that result in settlements, such as that filed by the University of California against Genentech for the company's manufacture and sale of the growth hormone product Protropin®, can be severe ($200 million in the case of UC vs. Genentech) punishments for the defendants[3].

That is not to mention the hundreds of thousands of dollars lost by both sides on legal and courtroom fees and on time spent by employees and management embroiled in the suit.

Although successful suits filed by small companies can result in large settlements or infringement damages from industry juggernauts, companies without the proverbial 'deep pockets' typically do not have the time and money to spend on lengthy, costly litigation. The price of resolving patent disputes can sometimes cripple a business, compared with the modest cost of building an effective IP portfolio. Thus, successful companies stand to benefit more from a strong IP portfolio to accompany equally strong and innovative research and development. Besides, with sound and successful innovation, a company can avoid being mired in litigation over a technology that it has long since improved upon.

From a different angle, those still questioning the value of intellectual property can look at the value derived from successful licensing of IP. The well-known Cohen-Boyer recombinant DNA patents, often credited as key catalysts of today's biotech industry, were reported to have earned $37.3 million in licensing royalties in 1997 alone[4].

While U.S. legislation such as the Bayh-Dole Act allowed for transfer of ownership of many government funded inventions from the U.S. government to the universities[5], resulting in successful licensing of almost half of university-born inventions[6,7], the fact is that an estimated 3% of all patents are actually licensed[8]. Thus an effective IP prosecution strategy should take note of the competing demands for licensing revenue and defense from litigious competitors. On one hand well-written patents are needed to defend the core technologies a company builds upon and on the other hand an aggressive patenting strategy is needed to map the course a company sees itself undertaking. The latter can result in licensing deals, or serve as a useful method for sidestepping unwanted litigation, by keeping far ahead of the competition.

Types of IP protection

- Patents
- Copyrights
- Trade Secrets
- Trademarks
- Licenses

Patents: United States patents offer protection for any process, machine, manufacture, or composition of matter, or any improvement thereof, that are novel, useful and

Corresponding Author: Dennis Farnandez, Fermandez and Associaties, LLP, 0147 El Camino Real Suite 201, Menlo Park, CA 94025, USA E-mail: osama@iploft.com

non-obvious[9]. The agreement in Trade-Related Aspects of Intellectual Property Rights (TRIPS agreements) in 1994, a multilateral concord proposed by the council administering the WTO's intellectual property agreement[10], defines patentable matter as any invention that involves an innovative step and has a potential industrial application[11].

In theory, the purpose of intellectual property is to foster intellectual and economic growth. Patents spur innovation through the disclosure and teaching of the details of an invention to the public and in exchange, the inventor or owner is rewarded the legal rights of ownership. The legal rights give the owner exclusive rights to capitalize on the invention, by excluding others from making or using the invention, importing the invention into the U.S., or offering the invention for sale. These ownership rights are granted for a period of 17-20 years, depending on the date of filing of the patent.

Patents are obtained through a lengthy process that can sometimes turn out to be quite costly. In high-tech fields such as biodefense and biosecurity technology, the time between filing a patent and a first response from the U.S. patent office is typically a year and a half. This is due in part to the large volume of patent applications in these fields and to the lack of expertise in the patent examiner corps. In Europe, Japan and the Pacific, the "first to file" system applies. On the other hand, in the U.S. the "first-to invent" system applies, but patent applications must be filed within one year of the first offer for sale of the product or the patent filing will be void. Thus it is important to keep an accurate record of dates of invention as well as offers for sale or other public disclosures.

Copyrights: Copyrights protect the original expression of an idea. By offering protection, copyright encourages the expression of original, artistic ideas into a tangible medium. Legal protection is effected instantly, when the original copyrightable subject matter is fixed into a tangible medium, e.g. on paper or in a digital storage form.

Copyrights are free and do not require months of paperwork as do patents and they are valid for the author's lifetime plus 50 years. A longer period of validity (75-100 years) applies if the work was created for hire, which is generally the case in a business involved in the high-tech industry.

Trade secrets: Trade secrets are any technical or business information that give a company a competitive advantage. There is no formal filing procedure to register trade secrets. The secret need not be completely novel or exclusive; it simply must have a derived or potential economic value from being unknown. Additionally, reasonable efforts must be made to keep the information secret, e.g. through the inexpensive use of Non-disclosure Agreements (NDA). Legal protection under trade secret no longer applies when the information is publicly disseminated.

Trademarks: Trademarks refer to the distinctive signature mark that can be used to protect the company, product, service, name, or symbol. The trademark must not be descriptive or generic. Legal protection is not offered to the technology, rather to the company good will and quality associated with the use of the recognized name or symbol. Trademarks provide exclusive rights within a region or nation and as long as used commercially and they may be renewed indefinitely. Compared to patents, they are obtained within a moderate time period (usually under two years) and typically at a cost under $5K per registered mark.

Licenses: Patents, trademarks, copyrights and trade secrets can all be licensed to a third party, giving that party permission to use the IP. Licenses generally fall in to three categories: exclusive, sole, or non-exclusive[12]. Only the licensee can exploit an exclusive license, while both the licensee and the licensor can exploit a sole license[12]. The licensor and an unlimited number of licensees can exploit a non-exclusive license[12].

Importance of intellectual property in security and privacy

Emerging technologies: In the US Government's concerted effort to develop and/or fund the development of high-tech applications for defense and security, there is likely technology that is classified as top secret that is much more advanced than the public is aware. Such technologies are beyond the scope of this study. There are, however, progressive technologies currently being developed in the public and private business sectors that are not so suppressed. Some of these are discussed below.

Biometrics: Biometrics, the technology of automatic personal identification via distinguishing physical attributes, emerges as another promising area for IP protection. The market for solid-state fingerprinting devices, retina scans, voice recognition and audio/visual data mining equipment used to analyze tone of voice and detect nervousness is starting to expand[13]. According to a recent report from the International Biometric Group, total biometric revenues are expected to grow rapidly through 2005, with the greatest gains in computer and network access and e-commerce[14]. These biometric

technologies have been proposed to ensure safety in public schools and will apply to security for such locations as the classroom, the school library and even on the buses and trains that the students use to get to school[14]. Some state legislatures are considering a bill that would require anyone applying for a state driver's license to provide one or more biometric identifiers-fingerprints, retina scans or scans on facial-recognition[15]. This demand by local governments would provide a large market for hardware and software that enables such biometric information to be easily attained and managed.

Currently, finger Scanning, is the leading biometric technology, with almost half the market, followed by facial then hand scanning[14]. Challenges in the market are minimal as the incidence of biometric forgeries-particularly of the fingerprint and retinal kind-are extremely difficult[16]. However, research from the School of Information Technology and Engineering (SITE) at the University of Ottawa, Ontario, Canada has stressed the possibility of regenerating identifiable images with important security and privacy implications for the use and storage of biometric data[17]. Thus, research and development efforts in optical technology, the manufacturing of indestructible hardware and algorithm scanning and processing to improve authentication accuracy rates[14] can direct entrepreneurs with inventive solutions to valuable IP protection. Biometrics also requires additional hardware, such as fingerprint readers or eye scanners and associated software where inventive improvements can be valuable.

A forecast of biometric revenues through 2006 for an overall compound annual growth rate (CAGR) of 54%, attaining market levels near $900 million[14], encourages that an aggressive market strategy and business plan alignment could provide the foundation for exclusivity in this market, yielding licensing revenue of non-core technology. For these types of distributed systems, architecture patents are more valuable compared to a specific implementation patent, since architecture patents are broader, providing the inventor with more infringement coverage.

Surveillance: With the US government increasingly tending towards eavesdropping on voice/online conversations and investing in data-mining efforts such as the Total Information Awareness (TIA) project and with foreign laws such as those requiring ISPs to keep email records for extended periods of time, an increasing number of companies will develop surveillance technologies to be sold to governments. The TIA system is sponsored by the Defense Advanced Research Projects Agency (DARPA) and is designed to search out terrorist clues before an attack and decode them prior to the assault[18]. TIA directors are hoping for "revolutionary advances in science, technology or systems and development of collaboration, automation and cognitive aids technologies that allow humans and machines to think together about complicated and complex problems" that will allow for the current feasablitibty of the TIA[14]. These technologies will include data-mining algorithms for data, voice and video information, firewalls and intrusion detectors, encryption/decryption techniques, massive storage systems, etc. implemented in software and/or hardware. One TIA project, called the HumanID Program, will be able to automate biometric to identify threats from great distances[19].

On the other hand, technologies emerge to counter "Big Brother" and ensure citizens' privacy. Examples involve the National ID controversy, unbreakable encryption schemes, untraceable and self-destructing email/publications, Virtual Private Networks (VPNs), anonymous Internet browsing and eavesdrop detectors that will enable citizens to live privately in and out of cyberspace. Consumer demand for these technologies will increase harmoniously with the government's increasing surveillance of what citizens consider private. IDC reports that the total IP VPN market will explode from $5.4 billion in 2001 to nearly $14.7 billion in 2006[20]. The biggest issue in this area concerns the bottleneck of information that various devices gather without an efficient means of analysis to transform the information into a meaningful interpretation. Entrepreneurs who can solve the informational logjam riddle by developing new applications for these technologies and can secure the associated patents-will be richly rewarded. With the high demand for these technologies that will likely occur, the probability that competitors will want to practice the associated patents is high, thus adding extra value to these registered patents.

With the US government's constant concern about homeland security, it is not surprising that the surveillance business continues to expand[21]. Although sophisticated cameras, such as those technologies that use Internet connectivity, only make up about ten percent of the surveillance market today, they are growing at 30 percent a year, twice the rate of standard security cameras and it is expected that by 2005, the market could surpass $500 million in the U.S. alone[21]. The U.S. currently has about ten million closed-circuit TV cameras for surveillance[22]. However, these cameras are largely analog cameras built with antiquated technology whereby automation is impossible[22]. Thus, there is a need of turning to digital technology and considerably developing video surveillance capability.

The US Government's push to increase national security has created many applications for biometric devices, which have traditionally been used in local and small-scale security settings. The foundation for still video cameras used for biometric recognition has heretofore been set and an application for video-face recognition was used for security in recent Super Bowls. It is, however, a relatively untouched emerging market and thus an abundance of patentable applications has yet to be discovered[23]. Such video-image recognition and processing can be expanded to diverse architectures for gathering video images-such as utilizing a number of cameras distributed over an area connected with algorithms that combine the images from the cameras to reconstruct the larger scene of the covered area. Surveillance cameras can be converted into real time sensor and information systems, enhancing real time security by processing image recognition algorithms into automated video surveillance devices[23] (Fig. 1). With the existence of prior art in this area already, IP strategies range from focusing on architectural patents and anticipating emerging security standards to expediting the patent examination process by identifying claims that have national security implications.

Such distributed architectures and algorithms for image/video stream extraction, along with the accompanying software and hardware needed to perform these algorithms will provide a plethora of valuable patents to the entrepreneurs that develop them. Patenting protocols between relevant nodes, in addition to the software and hardware of local nodes, can provide a source of licensing revenues.

These state-of-the-art technologies will be in want of new equipment capable of fast and efficient data-mining

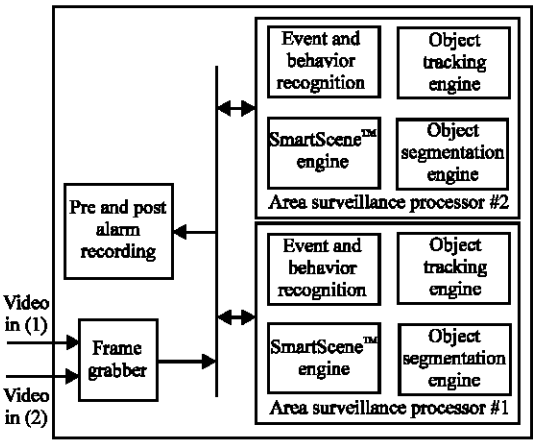

Fig. 1: Automatic visual monitoring server's duel channel area surveillance processor developed by MATE-CCTV[23]

techniques required for searching and storing large image/video repositories. The systems would also require new hardware architectures for implementing such storage/data-mining along with related communication protocols among nodes in such architectures, both of which, if developed, will provide valuable patents. Because process methods are patentable, the scheme associated with storing and/or searching algorithms could be patented as well.

Biological detection: With the constant threat of bioterrorist acts, the ability to detect various types of biological and chemical contaminants is vital to preventing human sickness. The conventional approach to microbial detection involves a variety of different methods to determine species type and to diagnose viruses and bacteria[24]. Samples taken from the environment, such as air, soil and water, typically must be cultured in a laboratory in order to obtain sufficient numbers of various cell types for reliable identification and the associated time required for microbial outgrowth can be up two days[24]. New amplification technology embodied in handheld Polymerase Chain Reaction (PCR) units can provide a more efficient process. These units feature disposable cartridges containing all necessary reagents, reaction chambers, waste chambers and microfluidics to extract, concentrate, amplify and analyze nucleic acids in the field[24]. These easy to use devices will be helpful to Hazmat teams and other emergency responders seeking to test the contents of a suspicious package for the presence of biological agents such as anthrax[24].

Currently, biodefense is challenged by the lack of real-time environmental detectors, such as biosensors, for potentially harmful biological agents[25]. Biosensors are devices that detect, record and transmit information regarding a physiological change or the presence of various chemical or biological materials in the environment[26]. For example, researchers at Virginia Commonwealth University are developing a fully integrated biochip system that enables the rapid detection, subspeciation and quantitation of biological agents[27]. The chip single-handedly prepares, analyzes and identifies a sample in real-time. This technological need beckons for IP rights in the improved development of biosensors and its components, such as a sensing elements, transducers, signal generators and data processors or microchips. In addition to detection elements, inventive opportunities arise in the advancement of intelligent diagnostic, computational, modeling or simulation software tools that can accurately identify environmental contaminants and minimize false

positives. There is a need for the development of next-generation systems for environmental detection, medical diagnostics and therapeutics that provide broader analysis and identification of agents of concern[25]. Thus, lucrative inventive opportunities not only exist for scientists developing medical countermeasures, but also for those in the medical device, software and semi-conductors industries able to develop other crucial functional or complementary components.

Military applications: The military often plays an important role when the task of biodefense is taken to other lands. The steady growth of the military-industrial complex will continue to fuel innovation in electronics, such as low power components, fuel cell vehicles, wearable devices, mobile broadband, low cost cameras, signal processors and artificial intelligence systems. Pertinent navigation systems include GPS-to-live-image translation, which already allows for the superimposition of weather images for real-time weather reports. Other GPS applications include, real-time vehicle tracking and monitoring systems capable of motion detection or live video that electronically relay information from thousands of miles away. Other opportunities arise in cybersecurity. The National Center for Advanced Secure Systems Research, launched with an initial $5.7 million investment, is developing projects that safeguard the computing and networking tools available to the military[28]. For example, these projects include developing better ways to monitor network security to prevent cyber attacks via computer worms and viruses and the creation of radios that will allow emergency personnel from crisis response agencies to communicate more effectively[28]. Patent strategies include expediting USPTO's examination process for IP relating to national security and low-cost provisional filings to ensure early filing dates followed by DARPA fundraising.

Nanotechnology: Perhaps the most intriguing area of technological advancement is in nanotechnology. Biochemical detection systems are being developed with biosensors that can detect and track minute amounts of strains and viruses. The newest technologies include nanoparticle medicines with faster delivery and improved control[28]. This efficiency is beneficial particularly with the ever-present threat of biological attacks in our large cities. Such an attack with chemical/biological agents would require a quick counter-action defense that nanoparticle medicines are able to provide[29]. Nanometer-scale traps can be developed that will be able to remove pollutants from the environment and deactivate chemical warfare agents[29]. On the other hand, research of the use of nanoparticles in the storage and delivery of pharmaceuticals and vaccines can lead to improvements in weaponization and the storage of biological warfare agents[25]. Current microencapsulation technology is focused on the development of processes to encapsulate biologically active organisms, proteins and even DNA within a coating nanoparticle substance[25].

It has been predicted that future advances in nanoparticle medicines are inevitable and that healthcare will be revolutionized by combining nanotechnology with biotechnology to produce ingestible systems that will be harmlessly flushed from the body if the patient is healthy but will notify a physician of the type and location of diseased cells and organs if there are problems[29]. Another important strategy is to project the emerging industry standards in this field in order to determine how inventions can utilize compatibility amongst entities in an exclusive, advantageous manner.

Other emerging devices in nanotechnology may include entire computer systems on a chip and nanoparticle reinforced materials[29]. In the effort to provide a faster, lighter weight military force, the government is very interested in quantum computers that use nanotechnology (Fig. 2). These systems promise enormous computational advance: 100 quantum particles can do the work of 1,000,000,000,000,000,000,000 of today's best computers[29]. Cutting-edge quantum science experiments are the foundation of this new technology and investigations into methods for fabrication of large-scale devices have started at Los Alamos National Laboratory[29].

The government is also exploring nanoparticle reinforced materials which are stronger, tougher and lighter than the current materials used on tanks (Fig. 3) and other armored vehicles used by the military[29].

Entrepreneurs in the emerging field of nanotechnology may lose IP rights by procrastinating the investigation of patent potential in nanotechnology until

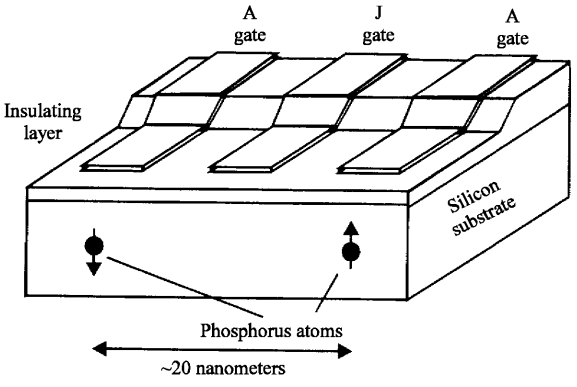

Fig. 2: One proposed quantum computer architecture[29]

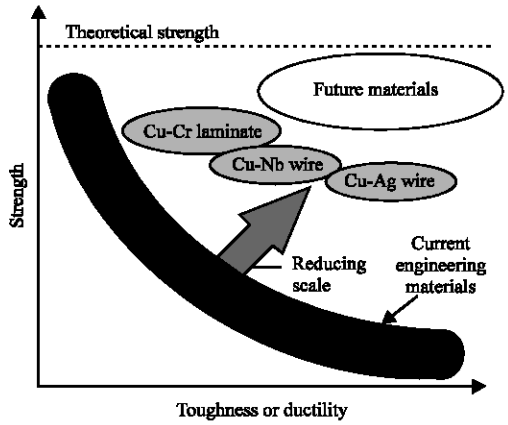

Fig. 3: Nanostructured materials can transcend the limits of strength and ductility of current engineering materials[29]

it is too late[30]. Patent coverage should be broad so that competitors have difficulty in avoiding the patent[30]. Because nanotechnology is relatively young, it is unlikely that the patent features in this area will be obsolete before the patent issues. On the contrary, it is logical to conclude that basic features and operating methods for nanotechnology patents will be around for several years. For complex systems such as these, which may require many elements playing together, inventors should consider patenting modules as opposed to patenting one large system. This is because it is likely that modules will be manufactured and/or used by different parties and the goal to is to prevent such individual infringers. If the complex system alone is patented, no single module manufacturer or user will be infringing.

As opposed to the sole benefit of a "defensive" patent, i.e., a patent that protects the core technology from rival entities, an offensive strategy should be implemented to maximize IP value. This approach entails the consideration of an effective business plan alignment, adequate research of competitor technology, partner IP rights positioning and/or acquisition, enforcement models, business methods and platform development.

The more successful patents are the ones that provide the requisite mix of claims that "push the boundaries of conventional practice, along with conventional types of claims" to generate a strategically successful IP right[31]. With this in mind, it must be remembered that patent applications must be enabling. Experts agree that valuable patents are frequently invalidated for lack of enablement[32].

Entrepreneurs should remember to include more than the minimal essential subject matter when drafting patent applications so that there is sufficient flexibility for creative arguing and claim expansion during patent prosecution and patent litigation[31]. One expert has noted that evolutionary changes in technology and what is considered to be patentable has given rise to the opportunity to obtain exclusive rights to technology in software and business method areas, previously thought to be excluded from patent protection[31]. Strategies that have challenged these exceptions to patentability have been richly rewarded and so a successful patent strategy includes stretching the boundaries of conventional practice as mentioned above[31]. For all types of possible devices, protocols, systems and methods, inventors should have the objective to patent the original idea and/or technology and then imagine future technologies enabled by their original material and patent those as well.

CONCLUSIONS

In its intellectual property portfolio, all companies should aggressively protect their core technology in numerous facets such as patent protection, copyright, trademarks and trade secrets. This is especially important in the high tech arena because as the demand for security and privacy necessitates the development of advanced applications, the quantity of protectable IP for the companies that develop the technologies will similarly increase. In addition to a defensive strategy of defending its core technology, companies should also pursue an offensive strategy that includes analyzing emerging standards and competitor focus so that companies could acquire a competitive advantage or entice a cross-licensing of another's technology.

REFERENCES

1. Chow, M. and D. Fernandez, 1999. Intellectual property strategies in bioinformatics. Fernandez and Associates LLP, 1999, http://www.iploft.com/articles2.htm#article2.
2. Rivette, K.G. and D. Kline, 2000. A hidden weapon for high-tech battles. Upside, pp: 165-174.
3. Kude, T., 1999. Regents drop case against genentech, agree to settle. UCLA Daily Bruin Online 22 Nov. 1999. http://www.dailybruin.ucla.edu/db/issues/99/11.22/news.settlement.html
4. Stanford Office of Technology Licensing, 1998. Medical staff update. http://wwwmed.stanford.edu/shs/update/archives/dec1998/fact.html
5. Consumer Project on Technology, 1999. The bayh-dole act. http://cptech.org/ip/health/bd

6. Campbell, K.D., 1998. TLO says government research pays off through $3 billion in taxes. MIT Tech Talk. http://web.mit.edu/newsoffice/tt/1998/apr15/patents.html
7. Council on Governmental Regulations, 1999. The Bayh-dole act: A guide to the law and implementing regulations. http://www.cogr.edu/bayh-dole.htm.
8. Murtha, E. J., 2001. Interview. Licensing Economics Review.
9. 35 U.S. Code, Sect. 101, 102, 103.
10. World Trade Organization, 1995. Overview: The TRIPS agreement. http://www.wto.org/english/tratop_e/trips_e/ intel2_e.htm
11. McCabe, K.W., 1998. Review of the TRIPS Agreement: Diverging views of developed and developing countries toward the patentability of biotechnology. J. Intl. Prop. L., 6.1: 41-67
12. Woodbridge, R.C., 1997. How to Negotiate a strong patent license. http://www.njiplaw.com/pdfs/license.pdf
13. Lowe, S., 2003. Fingerprinting and retina scans eyed up for schools. The Sydney Morning Herald. http://www.smh.com.au/articles/2003/01/13/1041990232082.html
14. FindBIOMETRICS.com, 2001. Biometrics: The anatomy lesson. http://www.findbiometrics.com/pages/feature%20articles/anatomy.html
15. Thibodeau, P., 2002. Congress eyeing uniform driver's license standards. Computer World. http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,70214,00.html
16. Davis, M., 2000. Biometric ID technology keeps an eye on your security authentification needs. Insight Magazine, http://insight-mag.com/insight/00/08/art-06.htm
17. Adler, A., 2003. Sample images can be independently restored from face recognition templates. Canada Conference on Electrical and Computer Engineering (CCECE), http://www.site.uottawa.ca/~adler/talks/2003/FaceRec-Regenerate-image-CCECE03-7may2003.pdf
18. Borin, E., 2002. Feds open 'Total' tech spy system. Wired News, http://www.wired.com/news/conflict/0,2100,54342,00.html
19. DARPA Information Awareness Office, 2000. Human ID at a distance (Human ID). http://www.darpa.mil/iao/HID.htm
20. Web Host Industry Review, 2001. IP-VPN market will grow to $14.7 Billion in 2006. IDC Says. http://thewhir.com/marketwatch/idc1218.cfm
21. Takahashi, D., 2003. Smart camera changing. The Face of security. San Jose Mercury Times. http:www.itsa.org/ITSNEWS.NSF
22. Cringely, R.X., 2003. The eyes have it iris recognition could mean the end of physical privacy, I, cringley the pulpit. http://www.pbs.org/cringely/pulpit/pulpit20030515.html
23. MATE-CCTV, Ltd., Products: AVMS 2000. http://www.mate.co.il/allproduct.html
24. Institute of Medicine and Board on Environmental Studies and Toxicology, 1999. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response, National Academy Press, Washington D.C., pp: 91-93, http://books.nap.edu/books/0309061954/html/91.html#pagetop
25. Petro, J.B. *et al*., 2003. Biotechnology: Impact on Biological Warfare and Biodefense, Biosecurity and Bioterrorim: Biodefense Strategy, Practice and Science, 1, No. 3.
26. Jacobson, K.B., 2003. Biosensors and other medical and environmental probes. http://ornl.gov/ORNLReview/rev29_3/text/biosens.htm
27. Guiseppi-Elie, A., 2003. Fully integrated biochip system for biodefense. IDHS Research Summit. www.idhs.org/summit/06-25-03-vcu-guiseppi.pdf
28. Emery, G.R., 2003. Supercomputing center to lead cybersecurity research effort. Washington Technology. http://www.washingtontechnology.com/cgi-bin/udt/im.display.printable?client.id=wtdaily-test&story.id=21088
29. Los Alamos National Laboratory, 1999. What is nanotechnology? http://www.lanl.gov/mst/nano/definition.html
30. Smith, E., 1997. When to patent: A framework for strategic business decisions. http://www.netpreneur.org/advisors/ip/wtpatent.html
31. Lytle, B.L. *et al*., 2000. Devising a patent strategy. 4th Annual Meeting of the National Collegiate Inventors and Innovators Alliance, http://www.nciia.net/proceed_01/Devising A Patent Strategy.pdf
32. Roe, K., 2003. Raising cash from patent and other IP portfolios for cash-strapped or bankrupt companies. Entrepreneurial Thought Leaders Seminar, Stanford University.