Intellectual Property Strategies in Security and Privacy

Dennis Fernandez; David Kemeny; Behfar Bastani
Fernandez & Associates, LLP.
1047 El Camino Real, Ste 201
Menlo Park, CA 94025
dennis@iploft.com; dkemeny@scu.edu; behfar@iploft.com
www.iploft.com

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 paper highlights some Intellectual Property (IP) strategies to successfully navigate the competitive landscape of these technical industries.

With the US government increasingly tending towards eavesdropping on voice/online conversations and investing in data-mining efforts such as the Total Information Awareness project, and with foreign laws such as those requiring ISPs to keep email records for extended periods of time and to facilitate decryption of records by authorities, an increasing number of companies will develop surveillance technologies to be sold to governments. Such 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. 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. 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 which 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 [1]. 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.

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 [2]. 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 [id.] (see Figure 1 below). 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 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.

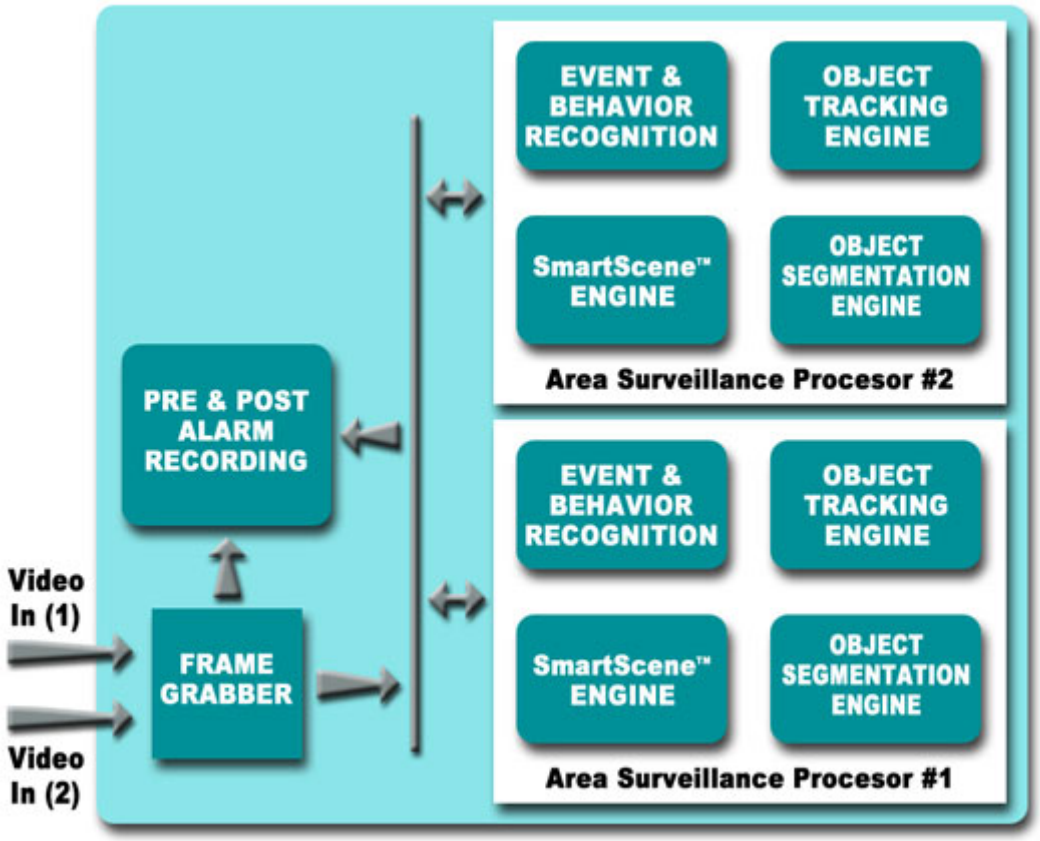

Figure 1: Automatic Visual Monitoring Server's Duel Channel Area Surveillance Processor developed by MATE-CCTV [2].

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. 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 [3]. 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. 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. 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. The reason is that architecture patents are broader, providing the inventor with more infringement coverage.

Tele-medicine, tele-justice, e-government (such as online taxes and USPTO communications), and emerging services such as gene databases have inherent privacy requirements which will require development of streamlined technologies such as secure databases, data exchange and authentication, and “blind” search and retrieval of database records. IP strategies here include claiming separate inventive pieces working in a network as opposed to claiming an entire configuration, as well as claiming protocols in addition to just “gadgets”. Because these technologies will impact the online industry, the associated patent claims will not likely go unnoticed.

Increasingly, businesses are installing Intellectual Property “trackers” which aim to tag or track company owned IP in order to prevent theft. This is an issue to both big companies who by their sheer size have trouble keeping IP in-house, as well as small companies who often don’t have much more to protect than their IP. Examples in this area include technologies for electronic watermarking and time-stamping. Entrepreneurs in this area can focus on technology that is unpredictable enough to foil hackers and other would-be intruders, as well as inventions which inter-operate with existing document handling systems already in use, and on drafting patent claims which encourage licensing.

The steady growth of the military-industrial complex will continue to fuel innovation in electronics, such as low power components, 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. 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.

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 & viruses. The newest technologies include nanoparticle medicines with faster delivery and improved control [4]. 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 may be able to provide. Nanometer-scale traps can be developed that will be able to remove pollutants from the environment and deactivate chemical warfare agents [id]. It has been predicted that future advances in this area 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 [id.]." 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 [id.]. In the effort to provide a faster, lighter weight military force, the government is very interested in quantum computers that use nanotechnology. These systems promise enormous computational advance. For example, 100 quantum particles can do the work of 1,000,000,000,000,000,000,000 of today's finest computers (see Figure 2 below) [id.]. 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 [id.].

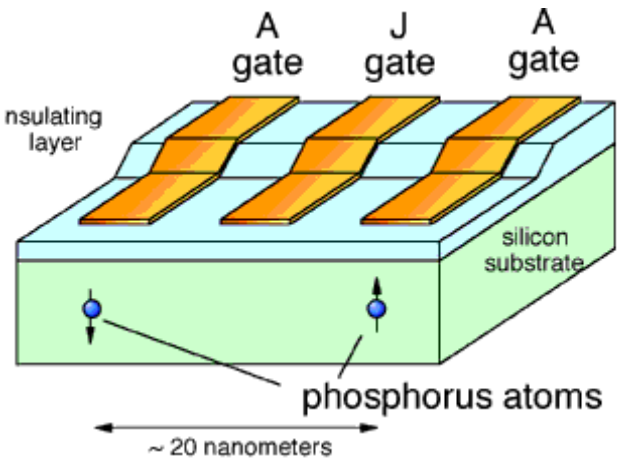

Figure 2: One proposed quantum computer architecture [4].

The government is also exploring nanoparticle reinforced materials which are stronger, tougher, and lighter than the current materials used on tanks and other armored vehicles used by the military.

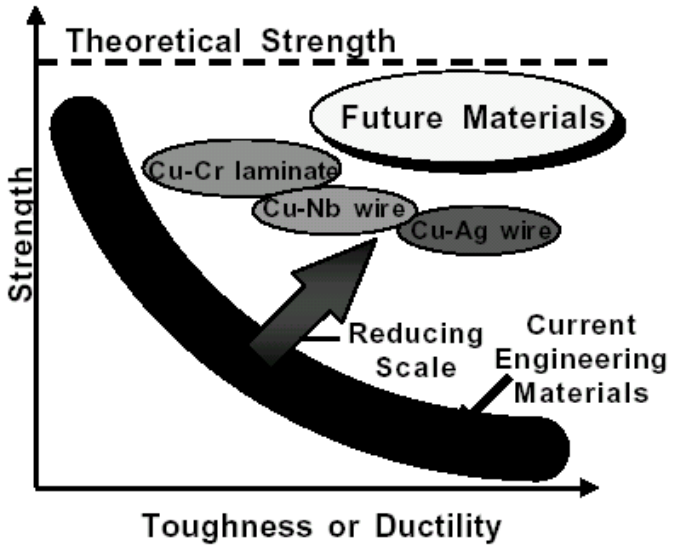

Figure 3: Nanostructured materials can transcend the limits of strength and ductility of current engineering materials [4].

Entrepreneurs in the emerging field of nanotechnology may lose IP rights by procrastinating the investigation of patent potential in nanotechnology until it is too late [5]. Patent coverage should be broad so that competitors have difficulty in avoiding the patent [id.]. 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 which "push the boundaries of conventional practice, along with conventional types of claims" to generate a strategically successful IP right [6]. 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. [7]
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 [8]. 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" [id.]. 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 [id.]. 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.

References:

[1] VPN Labs, *IP VPN Services: U.S. Market Forecast and Analysis, 2001-2006*, October 1, 2002, *available at* http://www.vpnlabs.com/vpn-categories/Market-Research/143/index.html

[2] MATE-CCTV, Ltd., *Products: AVMS 2000*, *available at* http://www.mate.co.il/allproduct.html

[3] Sue Lowe, *Fingerprinting and retina scans eyed up for schools*, The Sydney Morning Herald, January 14, 2003, *available at* http://www.smh.com.au/articles/2003/01/13/1041990232082.html

[4] Los Alamos National Laboratory, *What is Nanotechnology?, at* http://www.lanl.gov/mst/nano/definition.html

[5] Evan Smith, *When to Patent: A Framework for Strategic Business Decisions*, 1997, *available at* http://www.netpreneur.org/advisors/ip/wtpatent.html

[6] Bradley D. Lytle, et al., *Devising a Patent Strategy*, 4th Annual Meeting of the National Collegiate Inventors and Innovators Alliance, March 9-11, 2000, *at* http://www.nciia.net/proceed_01/Devising A Patent Strategy .pdf

[7] Kevin Roe, *Raising Cash From Patent and Other IP Portfolios for Cash-Strapped or Bankrupt Companies*, Entrepreneurial Thought Leaders Seminar, Stanford University, January 28, 2003.

[8] Bradley D. Lytle, et al., *Devising a Patent Strategy*, 4th Annual Meeting of the National Collegiate Inventors and Innovators Alliance, March 9-11, 2000, *at* http://www.nciia.net/proceed_01/Devising A Patent Strategy .pdf