THE Next Wave

The National Security Agency's review of emerging technologies

Access to innovation: NSA's Technology Transfer Program

Globe at a Glance | According to the Experts | Pointers

THE Next Wave
The National Security Agency's review of emerging technologies

GUEST Editor's column

Marian J. Roche

The National Security Agency's (NSA) Technology Transfer Program (TTP) was created in 1990, under the authority of the Technology Transfer Act of 1986. The TTP provides a venue for NSA inventors to share federally funded intellectual property and to conduct collaborative research with private industry, academia, nonprofits, other federal agencies, and state and local governments. The TTP is managed by the Technology Transfer Office located within NSA's Research Directorate.

Technology transfer can take on many different forms from licensing patents to providing scientific personnel in training and mentoring roles. However, collaboration is the key to successful technology transfer, and NSA recognized early on the value of its partnerships as well as the benefit of collaborative research and development (R&D). As a result, NSA actively seeks partners who are willing to license or continue R&D on the technologies within its large portfolio of patents and intellectual property. This portfolio encompasses a broad spectrum of technologies and scientific disciplines but is mostly concentrated within NSA's key areas of expertise including acoustics, communications, advanced mathematics, computer technology, information processing, networking, security, microelectronics, optics, and signals processing. (See page 2 for expanded descriptions of these areas of expertise, including examples.)

NSA's TTP utilizes several mechanisms including the following:

- **Patent License Agreements (PLAs)**—The goal of a PLA is to provide the private sector with the opportunity to commercially develop federally funded research to promote economic growth and global competitiveness.
- **Cooperative Research and Development Agreements (CRADAs)**—A CRADA provides NSA and the collaborating partner the opportunity to engage in joint research and development efforts, sharing the risks and benefits.
- **Educational Partnership Agreements (EPAs)**—An EPA allows NSA to share its unique experience by providing training to personnel in the science and technology fields at all education levels.
- **Technology Transfer Sharing Agreements (TTSAs)**—A TTSA allows NSA to transfer technology to other government agencies while protecting its rights.

For expanded descriptions of the TTP mechanisms, see page 4.

Broadly speaking, federal technology transfer exists to cycle the benefits of federally funded R&D back into the US economy, bringing new products to market, creating jobs, and increasing the industrial base. However, NSA's TTP provides additional benefits for the agency, its employees, and its partners. The most notable benefit is the ability to collaborate with outside technical experts and resources to help accomplish NSA's mission-oriented activities. Other benefits include providing NSA facilities and equipment for R&D efforts and the opportunity for university researchers, educators, and students to gain valuable learning experiences from collaboration with leading NSA scientists and researchers.

Perhaps the most intriguing benefit for the inventors is the reward and recognition. Technology transfer legislation allows NSA employees to receive monetary rewards for filing patents and to receive a percentage of any royalty payments from licensees.

Technology transfer has been one of the cornerstones supporting the agency's mission for over 20 years. NSA's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer. NSA pioneered efforts in flexible storage capabilities, which led to the development of the tape cassette. NSA also made groundbreaking developments in semiconductor technology and remains a world leader in many technological fields.

If past successes are an indication of things to come, the future of NSA's TTP is very bright. Startling new technologies are being developed and the intellectual property portfolio is growing. New relationships and partnerships are being developed. At the National Security Agency, PLAs, CRADAs, EPAs, and TTSAs are industry's *access to innovation*.

For more information about technology transfer or the TTP, visit www.nsa.gov/research/tech_transfer, or contact us:

National Security Agency
Technology Transfer Program
9800 Savage Road, Suite 6541
Fort George G. Meade, MD 20755–6541
tech_transfer@nsa.gov

Marian Rocke

Director
Technology Transfer Program, NSA

Contents

2 NSA technology transfer: Access to innovation

6 Federal technology transfer legislation highlights

10 Intellectual property: What it is and how it benefits NSA

14 From Fort Meade to the marketplace: Successes in technology transfer

18 Technology transfer with the University of Maryland—regional partner, national implications

20 Bringing technology inside NSA

26 GLOBE AT A GLANCE

28 ACCORDING TO THE EXPERTS

30 POINTERS

33 SPINOUTS *New!*

The Next Wave is published to disseminate technical advancements and research activities in telecommunications and information technologies. Mentions of company names or commercial products do not imply endorsement by the US Government.

To receive printed copies of *The Next Wave*, please use the Internet address below and provide a mailing address and the number of copies requested. For more information, please contact us:

National Security Agency
Attn: RL U Managing Editor
Suite 6541
Ft. George G. Meade, MD 20755–6541

Vol. 19 | No. 3 | 2012

Access to innovation: Technology transfer

NSA's Technology Transfer Program (TTP) provides a venue for NSA scientists and engineers to share federally funded intellectual property and to conduct collaborative research with private industry, academia, nonprofits, other federal agencies, and state and local governments. The TTP transfers technologies encompassing a broad spectrum of scientific disciplines including:

Acoustics—NSA's acoustic technologies include methods for identification, extraction, and analysis of voice and voice signals. Additional technologies include foreign language voice recognition, duplicate voice identification, and methods of measuring voice enhancement.

Examples available for license:

- Method of comparing voice signals.
- Method of phone-based speaker recognition.
- Voice activity detector.

Communications—NSA's communication technologies include methods of transmitter geolocation, station synchronization methods, error correction, filters, equipment simulation methods, and novel speech transmission techniques.

Examples available for license:

- Method of correcting modem transmission errors.
- Method of locating a transmitter.
- Device for impedance matching radio frequency open wire transmission lines.

Advanced mathematics—NSA's advanced mathematics technologies include computerized systems for solving nonlinear Boolean equations, cryptographic methods, random number generation, geometric pattern recognition, and methods to display complex mathematics.

Examples available for license:

- Method for solving nonlinear Boolean equations.
- Cryptographic method using modified fractional fourier transform kernel.
- Method for generating multiple random numbers.

Computer technology—NSA's computer technologies include advanced software techniques as well as novel hardware input/output devices.

Examples available for license:

- Method of protecting a computer stack.
- Method of removing loops from a computer program.
- Method of monitoring multiple computer calls.

at NSA

Microelectronics—NSA's microelectronics technologies include water fabrication methods, specialty electronic circuits, methods to view magnetic patterns on magnetic media, and novel circuit board technologies.

Examples available for license:

- Method of making a thin, conformal, high-yielding, multichip module.
- Printed circuit board with RF absorber.
- Method for bumping a thin wafer.

Information processing—NSA's information processing technologies include methods to efficiently store, retrieve, and modify data in any language format, methods to extract text from graphics, optical character recognition, and authentication methods.

Examples available for license:

- Method of storing, retrieving, and modifying data in any language representation.
- Method of extracting text from graphical images.
- Method of biometric authentication.

Security—NSA's security technologies include methods of generating cryptographic keys, digital signature validation, secure computing technologies using virtual machines, as well as physical security devices.

Examples available for license:

- Self-authenticating cryptographic apparatus.
- Device for and a method of secure computing using virtual machines.
- Method of wireless intrusion detection.

Networking—NSA's networking technologies include advanced firewall technologies, multiple level minimum logic networks, traffic monitoring as well as inter-network data transport, secure file transfer, and network address location methods.

Examples available for license:

- Multiple level minimum logic network.
- Firewall for processing a connectionless network packet.
- Method for geolocating logical network addresses.

Optics—NSA's optical technologies include optical bandpass filters, optical switches, modulators, optical clock recovery, and beacon authentication methods.

Examples available for license:

- Acousto-optic bandpass filter.
- Device for modulating an optical signal using a single waveguide.
- All fiber optically controlled optical switch.
- Method of authenticating beacon.

Signal processing—NSA's signal processing technologies include transmitter location methods, range limited antennas, noise reduction techniques, amplification, frequency estimation, and signal decoding methods.

Examples available for license:

- Range limited antenna.
- Method of signal processing for determining range and velocity of an object.
- Method for removing noise and interference from a signal.

Technology transfer

To facilitate the transfer of technology to its partners, NSA's TTP utilizes several mechanisms including the following:

Patent License Agreement (PLA)

A PLA is a license granted by NSA to a partner to commercially develop and market its patents and patent applications. Using a PLA, NSA grants its partner a nonexclusive, partially exclusive, or fully exclusive license to make, use, or sell the patented invention. In return, the partner typically pays a royalty back to the government.

When a patented NSA technology is identified by a licensee as having commercial potential, the licensee submits a satisfactory development and marketing plan. This plan outlines the licensee's approach to commercialization of the invention. The invention must be brought to market within a specified time period and the licensee must continue to make the benefits of the invention accessible to the public.

A PLA is designed to maximize the use of NSA developed technology in the private sector. Benefits of a PLA include:

- Encouraging commercialization of federally funded research in the private sector.
- Saving industry and academia the cost and time of conducting research and development (R&D).
- Providing royalty income to the government and its inventors.
- Creating new industry and employment opportunities in the private sector.
- Maximizing the value of the NSA's R&D investment and resulting technologies.
- Increasing the awareness of market and technology trends and the needs of both industry and government.

Cooperative Research and Development Agreement (CRADA)

A CRADA is a cooperative agreement between NSA and industry, academia, nonprofits, and state and local governments. These agreements leverage each party's resources in order to conduct R&D that benefits both. Through this collaboration, each party shares the benefits and risks in obtaining valuable technology transfer goals and objectives.

A CRADA allows both parties to leverage personnel, facilities, equipment, and other resources during collaborative R&D activities. The nonfederal partner does not receive any funds from NSA, but may contribute funds to the project. Under a CRADA, the government may grant the nonfederal partner patent licenses for any invention developed under the agreement.

A CRADA is one of the most valuable technology transfer mechanisms for obtaining long-term value. The benefits of entering into a CRADA include:

- Creating new products, processes, and intellectual property to meet mission and commercial goals.
- Reducing research and development costs and time.
- Leveraging external expertise, ideas, and resources.
- Providing a joint approach to solve specific problems by applying different cultural solutions.
- Increasing the probability of bringing inventions to the marketplace.
- Increasing the awareness of market and technology trends and the needs of both industry and government.

mechanisms

Educational Partnership Agreement (EPA)

An EPA is an agreement between NSA and an educational institution to transfer or enhance technology and provide technology assistance to the institution. Under an EPA, NSA scientists can provide training and mentoring to personnel in the science and technology fields. Also, NSA may transfer or donate laboratory equipment to public and private schools.

An EPA is normally initiated by an NSA sponsor who submits the educational objectives for review. A task plan is developed in collaboration with the institution outlining the learning objectives and goals. These goals may be teaching, mentoring, training personnel, developing curriculums, or transferring equipment and technology. Once approved, both parties can begin executing the learning tasks.

An EPA is designed to formalize the relationship between NSA and an educational institution. Benefits of an EPA include:

- Involving students to ensure a future resource of scientists, mathematicians, and engineers.
- Providing unique opportunities for learning not available from other resources.
- Providing access to NSA personnel to teach courses and develop science curriculums.
- Permitting students and teachers to become involved in developing useful technological applications.
- Providing access to NSA resources, either by loan or donation, which relieves institutions from some of the financial burden of R&D investment.
- Improving community awareness of NSA core values and enhancing the reputation of the laboratory.

Technology Transfer Sharing Agreement (TTSA)

NSA has numerous patents, patent applications, and other intellectual property (IP) that it frequently transfers to other government agencies. A TTSA is an agreement between NSA and another agency that protects NSA's rights to seek commercialization of technologies it owns and to effectively track the transfer of these technologies.

A TTSA is initiated by NSA government personnel for the recipient agency. Each TTSA includes specific language regarding noncomercialization and restricts the transfer for government use only. Contractors and other partners requiring technology in support of a contract must have their Contract Officer Representative (COR) submit the request.

A TTSA is designed to simplify the transfer of technology between NSA and other government agencies. Benefits of a TTSA include:

- Simplifying agreements that specify the purpose, terms, and conditions related to the technology transfer.
- Facilitating easy transition of technology between US government agencies.
- Reducing recipient agency R&D expenditures by leveraging previous NSA investments.
- Reducing development time of mission-specific technologies.

For more information about technology transfer or the TTP, visit www.nsa.gov/research/tech_transfer, or contact us:

National Security Agency
Technology Transfer Program
9800 Savage Road, Suite 6541
Fort George G. Meade, MD 20755–6541
tech_transfer@nsa.gov

Federal technology transfer

Since the 1980s, Congress has enacted a series of laws to establish and provide technology transfer guidelines, mechanisms, and incentives for Government Owned and Government Operated (GOGO, e.g., The Army Research Laboratory) and Government Owned and Contractor Operated (GOCO, e.g., Sandia National Laboratory) federal laboratories participating in technology transfer activities. The following text summarizes major legislation and executive orders that directly focus on technology transfer activities.

Stevenson-Wydler Technology Innovation Act of 1980

This Act is the first of an ongoing series of laws that define technology transfer and encourage federal laboratories to engage in cooperative research with state and local governments, academia, nonprofit organizations, or private industry. Its provisions also establish and define the basic activities of an Office of Research and Technology Applications at each federal laboratory and set aside a small percentage of each laboratory's budget to fund technology transfer activities.[a]

Bayh-Dole Act of 1980

This Act permits universities, small businesses, and nonprofit organizations to obtain title to inventions developed with federal funds. However, this policy also allows the federal agency to retain an irrevocable, paid-up license to use the invention. It permits GOGO laboratories to grant exclusive patent licenses to industry.[a]

legislation highlights

Federal Technology Transfer Act of 1986

This Act amends the Stevenson-Wydler Act and codifies a number of changes that impact GOGOs. It requires scientists and engineers to consider technology transfer an individual responsibility and also requires that technology transfer efforts be considered in their performance evaluations. It also establishes the guidelines for inventors from GOGOs to receive monetary awards from royalty-bearing licensing agreements. GOGOs are given the authority to enter into Cooperative Research and Development Agreements (CRADAs); to license inventions that might result from such arrangements; to exchange laboratory personnel, services, and equipment with research partners; and to waive rights to lab inventions and intellectual property. Additionally, the Act allows for federal employees, both current and former, to participate in commercial efforts if there is no conflict of interest. It established the charter for the Federal Laboratory Consortium for Technology Transfer. The Consortium is responsible for a variety of activities including providing training courses and assistance for technology transfer programs.[a]

National Technology Transfer and Advancement Act of 1995

This Act amends the Stevenson-Wydler Act and ensures that federal laboratories grant collaborating parties sufficient intellectual property rights under CRADAs for prompt commercialization. It also provides guidelines for licensing and ownership of inventions resulting from joint research performed under a CRADA. Additionally, the law raises the financial rewards for federal employees whose invention results in a royalty-bearing agreement to the annual limit payment of $150,000.[a]

Executive Order 12591 of 1987

This Executive Order assures that federal laboratories can enter into CRADAs with other federal laboratories, state and local governments, universities, and the private sector. It also promotes commercialization of federally funded inventions by ensuring laboratories grant to contractors the title to patents developed with federal funds, as long as the government retains a royalty-free license for government use.[a]

Federal technology transfer

Technology Transfer Commercialization Act of 2000

This Act promotes the benefits of a CRADA and expands its licensing authority to permit federal laboratories to include preexisting government inventions to make CRADAs more attractive to private industry. It also mandates licensees of inventions to provide a development and/or marketing plan for the requested invention and to commit to achieving practical application in a reasonable period of time. It requires federal agencies to provide a 15-day public notice before granting exclusive or partially exclusive licenses to non-CRADA created or made inventions.[a]

America COMPETES Act of 2007

This Act authorizes programs in multiple agencies focused on the overarching themes of increasing funding for basic research; strengthening teacher capabilities and encouraging student opportunities in science, technology, engineering and mathematics (STEM) educational programs; enhancing support for higher risk, higher reward research; and supporting early career research programs for young investigators. The primary impact on technology transfer includes the elimination of the Department of Commerce Office of Technology Administration and the associated Under Secretary, which had the principal reporting and analytical responsibilities for technology transfer activities government-wide (these duties were reassigned within the Department of Commerce).[a]

References

a. Federal Laboratory Consortium for Technology Transfer. *The Green Book: Federal Technology Transfer Legislation and Policy.* 2009. Available at: http://www.federallabs.org/store/greenbook/

b. Jones G. President signs America COMPETES Reauthorization. *FLC NewsLink*. 2011 Feb 14. Available at: http://newslink.federallabs.org/2011/02/14/president-signs-america-competes-reauthorization/

c. Administration of Barack Obama. Memorandum on Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses. DCPD-201100803, 2011 Oct 28. Available at: http://www.gpo.gov/fdsys/pkg/DCPD-201100803/html/DCPD-201100803.htm

d. US House of Representatives Committee on the Judiciary. Background on H.R. 1249, the America Invents Act. 2011. Available at: http://judiciary.house.gov/issues/issues_patentreformact2011.html

legislation highlights

America COMPETES Reauthorization Act of 2010

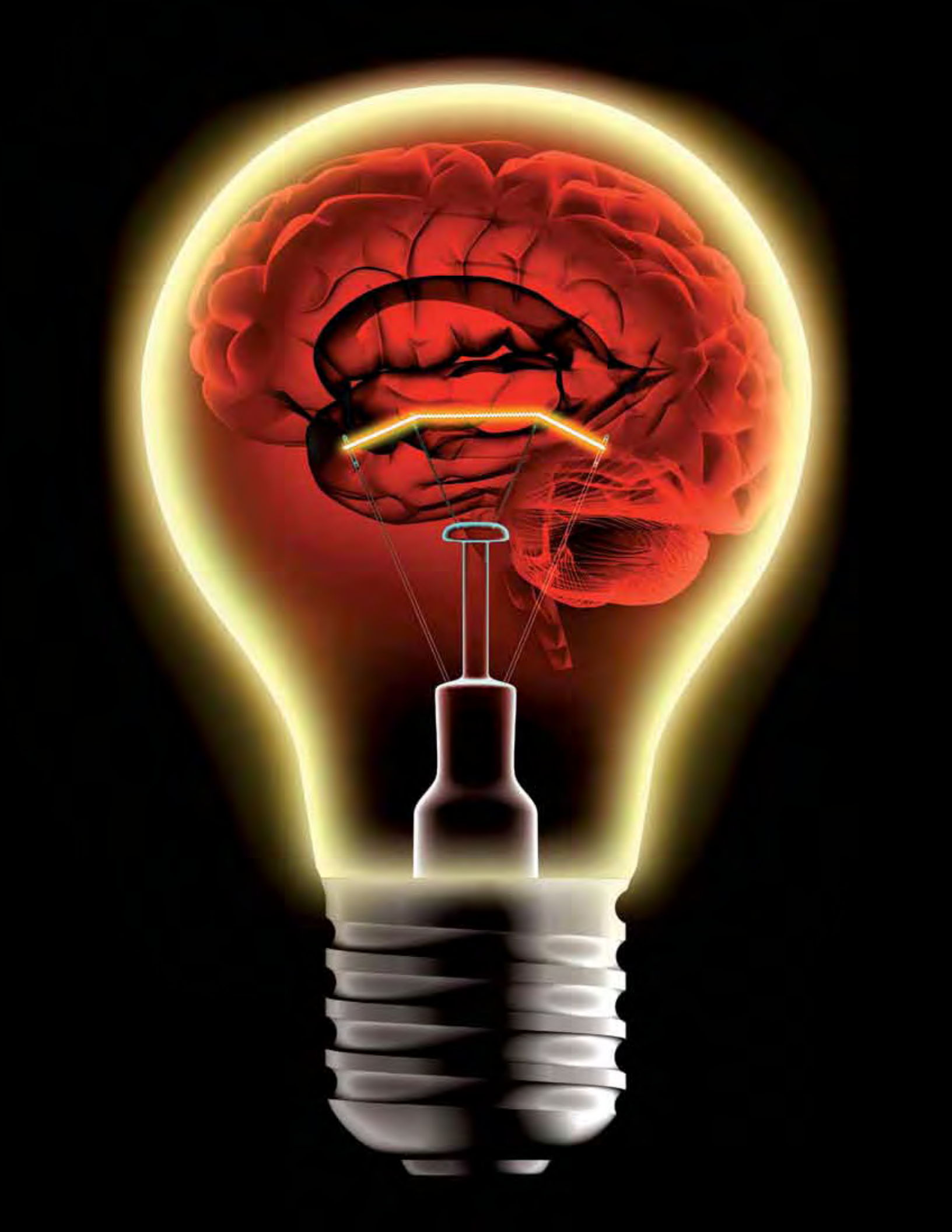
This Act reauthorizes selected provisions of the 2007 America COMPETES Act. It increases funding for physical sciences and engineering R&D and authorizes certain federal STEM education programs. Several provisions in the Act directly call out technology transfer. It authorizes federal agencies to award competitive prizes to stimulate innovation, formally establishes an office within the Department of Commerce to develop policies supporting commercialization of federally funded R&D, and establishes a regional innovation program. Federal labs are eligible for funding under this provision.[b]

Presidential Memorandum on Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses (2011)

This Memorandum directs each executive department and agency that conducts R&D to develop plans to establish performance goals to increase the number and pace of effective technology transfer and commercialization activities. Additionally, agencies are required to streamline their technology transfer and commercialization processes and to facilitate commercialization through local and regional partnerships with nonfederal entities, including private firms, research organizations, and nonprofit entities.[c]

Leahy-Smith America Invents Act of 2011

This Act implements a first-inventor-to-file standard for patent approval, creates a postgrant review system to weed out bad patents, and helps the Patent and Trademark Office address the backlog of patent applications. For more information, see page 31.[d]



Intellectual property: What it is and how it benefits NSA

In an era of rapidly changing technology, intellectual property has become a game changer and an important commodity, even within the government arena. What is intellectual property? Essentially, intellectual property is a creation of the mind that can be sold or copied. The United States Patent and Trademark Office (USPTO) defines intellectual property as "creations of the mind—creative works or ideas embodied in a form that can be shared or can enable others to recreate, emulate, or manufacture them." These creations typically fall into one of four intellectual property categories including patents, trademarks, copyrights, and trade secrets.

Patents

As defined by the USPTO

A patent is an intellectual property right granted to an inventor "to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States" for a limited time in exchange for public disclosure of the invention when the patent is granted. There are three kinds of patents including utility, design, and plant patents. They protect devices, methods, chemical formulas, aesthetic designs, and plants. The term of a utility or plant patent is 20 years from the filing date of the patent application. For design patents, however, the term is reduced to 14 years from the filing date of the patent application. In certain cases, the term can be extended due to delay in the patent examination process. (NSA primarily obtains utility patents on devices or methods, but, on occasion, NSA has also pursued design patents for aesthetic designs.)

At NSA

You may be surprised to hear that NSA seeks patents. However, many of the technologies developed by NSA not only satisfy mission requirements, but also have great potential for commercial use. Following extensive review, NSA may seek patent protection for such technologies as a way to protect and build on the US government's (USG) investment in research and development. Additionally, recent legislative changes will eventually result in the USPTO granting patents to the first inventor to file rather than to the first person to invent. This change will harmonize the US patent system with the patent systems used in almost all other countries. As a result, US government agencies, including NSA, must now take a more aggressive and proactive approach to patents than in the past.

Patent protection allows NSA to license its technology, which brings in funds to support further research and promotes economic development. NSA also has an interest in protecting itself against claims of patent infringement. Occasionally, the USG has invented a technology first but found itself as a defendant in a case of patent infringement because patent protection was not sought at the time of the invention. Seeking patent protection at the time of the invention is the most effective way of reaping the benefits of the USG's investment and of protecting itself from nuisance lawsuits.

Trademarks

As defined by the USPTO

A trademark is a word, phrase, slogan, symbol, design, or a combination thereof, that identifies and distinguishes the maker of a particular product or goods. Rights can be established based on use of a mark in commerce, without registration. Owning a federal trademark registration, however, provides many advantages including a legal presumption of ownership of the mark, the exclusive right to use the mark nationwide on or in connection with the goods/services listed in the registration, and the ability to bring an action concerning the mark in federal court. Unlike a patent, the term of a trademark lasts as long as the trademark owner maintains the trademark registration.

At NSA

NSA's ability to obtain a trademark is often hindered by the requirement that the mark be used in the stream of commerce. This requirement can often be overcome if the mark is or will be used with the public. Two examples of trademarks that NSA has successfully registered are Autoberry® and NetTop®.

Copyrights

As defined by the USPTO

A copyright is a form of protection provided to the authors of "original works of authorship," including literary, musical, dramatic, artistic, sound recordings, and certain other intellectual works whether the works have been published or not. All facts and any titles, names, short phrases, slogans, ideas, or works that have no originality are not copyrightable. At a minimum, copyright owners have the exclusive right to reproduce the work, prepare derivative works, distribute copies of the work, perform the work, and display the work. For works of an individual, the term of a copyright extends for the life of the author plus 70

years. On the other hand, for works of a corporation, the term of the copyright is 95 years from publication or 120 years from creation, whichever expires first.

At NSA

Usually, a work receives copyright protection as soon as pen hits paper. However, a work created by an NSA employee, or any USG employee, as a part of the employee's official duties is not entitled to copyright protection. Additionally, NSA is required to respect copyright law and must obtain permission to use copyrighted material in most cases. However, there are some exceptions that allow use of a copyrighted work without express permission from the copyright owner. One such exception often relied upon is the Fair Use exception. In determining if a proposed use is a "Fair Use," several factors are weighed including: (1) the purpose of the use, (2) the nature of the work, (3) the amount of the work that will be copied, and (4) the economic impact of the copying on the copyright owner.

Trade secrets

As defined by the USPTO

A trade secret consists of information and can include a formula, pattern, compilation, program, device, method, technique or process. To meet the most common definition of a trade secret, it must be used in business, and give an opportunity to obtain an economic advantage over competitors who do not know or use it. A trade secret holder is only protected from unauthorized disclosure and use which is referred to as misappropriation. If a trade secret holder fails to maintain secrecy or if the information is independently discovered, becomes released or otherwise becomes generally known, protection as a trade secret is lost.

At NSA

While most corporate entities manage this type of intellectual property, the USG maintains relatively fewer trade secrets. Within the government realm, trade secrets are considered to be Proprietary Information and the USG is required to protect it just as it would any other protected information.

From Fort Meade to the marketplace: Successes in technology transfer

The NSA Technology Transfer Program (TTP) has enjoyed many successes, but none more so than the technologies and companies highlighted here. This article illustrates a few of the more notable technology transfer efforts and the commercial companies that took on the challenge of bringing the technology to market.

AutoBerry—a game changer in mobile device security and assurance

With more than 1.8 billion smartphones expected to be in use by 2013, the security of these and other digital devices are of critical concern to national security and global commerce. Daryle Deloatch and Mark Haney, analysts in NSA's Information Assurance Directorate, have made a significant contribution to maintaining that security with their patented Method of Tampering Detection for Digital Devices, or AutoBerry.

AutoBerry rapidly scans digital devices in search of any anomaly that could indicate tampering or other malicious activity. By essentially "fingerprinting" each device, the scanning software extracts application and operating system files and compares the results to a known good baseline to reveal any changes.

The scan takes from 5 to 17 minutes depending on the device—a dramatic reduction from the 1.5 hours typically required to do a manual security check—and requires minimal technical training. As a result, security personnel, administrators, and other users can quickly identify devices that have been compromised and seek additional forensics support as necessary.

Enter Fixmo

Fixmo was a small start-up developing management and security applications for BlackBerry devices and had a booth at the 2010 conference of the Cellular Telecommunications Industry Association (CTIA). When Fixmo's Chief Executive Officer Rick Segal took a wrong turn on his way back to his booth, he accidentally stumbled upon the NSA TTP booth. As luck would have it, the TTP, along with inventors Haney and Deloatch, just happened to be demonstrating the AutoBerry technology in an effort to attract potential licensees.

On seeing the demonstration and meeting the inventors, Segal immediately expressed interest in exploring a licensing agreement. The inventors recognized that Fixmo was a "black belt" in BlackBerry application development. Segal then scheduled a two-day session with the inventors. "We were building the technology on our own, but after we met the NSA team at the show and learned more about their technology, we decided to abandon what we were doing and use the great work done by the NSA inventors," said Segal.

Although several companies expressed interest after seeing AutoBerry at CTIA, Fixmo quickly stood out as

the best potential partner. The company realized that as smartphones evolved into personal computers, the demand for management, monitoring, and security of mobile devices and enterprise infrastructure would skyrocket. Transfer of the AutoBerry technology occurred in just weeks.

Discussions between NSA and Fixmo began in March 2010 and an exclusive Patent License Agreement (PLA) and short-term consulting Cooperative Research and Development Agreement (CRADA) were signed in June 2010. Within 60 days, Fixmo had gathered user requirements from the existing customer base and started development of an upgraded version of the software.

Credit for this astonishing timeframe—unprecedented at NSA and unheard of in many other federal laboratories—goes in large part to the partners' shared vision of how commercialization would not only support but enhance the AutoBerry technology. The inventors and TTP realized that Fixmo had both the vision and the resources to take AutoBerry to the next level and provide enhancements, upgrades, and add-ons.

In February 2011, NSA and Fixmo entered into a second CRADA, enabling them to collaborate on the enhancement and development of a range of mobile enterprise and risk management technologies.

The impact

Fixmo's biggest impact on the product was the enhancement of AutoBerry from a manual communications security function that required tethering the device to a server to an "over-the-air" provisioned system providing real-time security services. This enhancement alone has resulted in huge man-hour and cost savings as well as enhanced security.

Fixmo has launched three versions of its Sentinel product line since the PLA was signed in June 2010:

- **Sentinel Desktop** is Fixmo's no charge product offering for government users that provides enhanced AutoBerry features for BlackBerry, Android, iOS, and Good devices. It is also available as a SteelCloud appliance.
- **Fixmo Sentinel™** is the flagship mobile risk management solution providing all of the advantages of Sentinel Desktop in an enterprise offering for government and industry.

Autoberry inventors receive tech transfer award

On May 3, 2012, the Federal Laboratory Consortium (FLC) presented Autoberry inventors Daryle Deloatch and Mark Haney with an Award for Excellence in Tech Transfer. The FLC award recognizes employees of FLC member laboratories who have accomplished outstanding work in the process of transferring federally developed technology.

The NSA engineers began developing AutoBerry in 2006 after being unable to find an automated tamper detection product on the market to speed up forensic analysis. Though they started working on their invention without knowing that they could patent and commercialize the result, Deloatch and Haney became determined champions when the technology transfer process got under way. In addition to working with a NSA patent attorney on submission of a patent application in 2008, both gave several company demonstrations to interested commercial partners. Deloatch also presented the technology at a day-long government technology showcase hosted by Johns Hopkins Applied Physics Lab in 2007 as well as at the CTIA show in 2010 where it drew the interest of several companies including Fixmo.

After the Fixmo PLA was signed, Deloatch and Haney quickly realized the potential of the partnership and strongly advocated for an expanded relationship. They continue to work closely with Fixmo to implement the current CRADA, frequently visiting or hosting the team to review customer recommendations and further additional research and development.

About the FLC: It was organized in 1974 and formally chartered by the Federal Technology Transfer Act of 1986 to promote and strengthen technology transfer nationwide. In consonance with the Federal Technology Transfer Act of 1986 and related federal policy, the mission of the FLC is to promote and facilitate the rapid movement of federal laboratory research results and technologies into the mainstream of the US economy. Today, approximately 300 federal laboratories and centers and their parent departments and agencies are FLC members.

- **Sentinel Server Compliance Check (SCC)** is Fixmo's newest product and is the commercial version of AutoBES, NSA technology developed under the CRADA that automatically audits, corrects, and confirms server configuration. Under the CRADA, Sentinel SCC is available at no charge for government agencies.

Fixmo now has more than 650,000 mobile devices under management with a customer base that includes many government agencies around the world as well as commercial enterprises. Its potential is staggering given that the mobile device management component of mobile risk management is a $300 million industry with a projected growth rate of 70 percent year-over-year.

Under the CRADA, the NSA inventors continue to work closely with Fixmo's technical team to enhance the existing technology and develop new, best-in-class, commercial off-the-shelf solutions for government implementation. To date, Fixmo has applied for three additional patents for Autoberry-related technology.

Former NSA engineer licenses NSA technology to form network analytics company

For 18 minutes on April 8, 2010, approximately 15 percent of all Internet destination traffic was routed through servers belonging to China Telecom. The reroute affected US government and military networks, including the the Office of the Secretary of Defense, the Department of Commerce, NASA, and the US Senate, as well as the Army, Navy, Air Force, and Marine Corps. Commercial sites, including those belonging to Microsoft, Dell, and Yahoo, were also affected.

Former NSA engineer Greg Virgin knows all too well how vulnerable network traffic can be. As one of the lead developer's of NSA's Analytic Metadata Producer (AMP) application, Greg has heard these stories all too often. AMP is a high-end, large-scale, analytical application used for network assurance. When AMP is coupled with TRICKLER, a passive network analysis tool, network administrators and security personnel can monitor data traffic and produce reports that can potentially identify threats, vulnerabilities, covert channels, insider threats, denial of service attacks, and spammers.

AMP is the metadata-producing sensor software that derives data for TRICKLER. AMP generates custom records of network traffic independent of specific network hardware and delivers more accurate data records with better precision and reliability than router-generated flow systems.

TRICKLER, on the other hand, efficiently and passively collects repetitive portions of network data and leverages that data to identify network assets without using signatures. The TRICKLER architecture consists of a front-end user interface and a knowledge base stored as MySQL metadata.

The TRICKLER knowledge base combines flow data for combination with operating system fingerprinting technology and a vulnerability database from the National Institute of Standards and Technology, called the National Vulnerability Database. Notable attributes of TRICKLER include the following:

- Robust handling of enormous data flows,
- A set of alarm files listing protocols detected on uncommon ports,
- A list of server and client banner strings pulled from set regions of common protocols, and
- A list of Internet protocol (IP) addresses exhibiting Internet relay chat botnet behavior.

When Virgin left NSA to form his own company, REDJACK, he licensed the AMP/TRICKLER technology from NSA. Virgin and his team continue to enhance and develop the product, for example, adding IPv6 functionality.

According to Virgin, "AMP now handles a number of new network protocols, network protocol encapsulation, as well as IPv6. Additionally, AMP now adopts a more advanced data format and postprocessing mechanism that allows for more flexible analytics and effective use of the data." REDJACK now provides the application to industry. When asked how well his product was working, Virgin replied, "Let's just say that AMP has enabled the detection of several

incidents and network activities that were previously undetected." As an example, one of Virgin's customers used AMP to discover that all of its Google traffic was being rerouted.

NetTop: One technology path—many roads to success

NetTop is a cross domain solution that provides access to multiple network domains with different classification levels from a single system over a single wire. NetTop integrates commercial off-the-shelf products to create multiple secure virtual machines utilizing mandatory access controls (MAC) based on Secure Enhanced Linux. Each virtual machine (VM) can be independently attached to a different network to provide complete isolation from other VMs running on the same system without compromising the security of any attached network. These operating systems may be fat or thin clients providing secure access to the cloud.

NetTop was unique from the beginning. According to inventors Bob Meushaw and Don Simard, the goal for NetTop was as much about developing new technology transfer approaches as it was about developing new technology. In order to provide potential licensees some level of protection, one of the first steps was to file a patent application to gain control of the intellectual property embodied in NetTop. (One of the original criticisms was that without intellectual property protection, there would be no competitive advantage to potential licensees.) In addition, NSA also decided to seek a trademark for the name NetTop; this would prove to be very useful in later phases of the marketing program. Having protected NetTop's intellectual property and name, the team began a search for industry partners capable of commercializing it. And to help with market development, the NetTop team used what was then a relatively new NSA program—the TTP.

Shortly after the decision to pursue a technology transfer path for NetTop through the licensing of the intellectual property, the NetTop team initiated a series of meetings with potential commercial partners. The most promising partner, initially, was the federal division of Compaq Computers. Compaq management saw potential in NetTop to help them build a market in security-related IT.

Discussions with Compaq were positive but were soon interrupted because of a possible merger with HP. After the merger in 2001, discussions resumed with the new federal division of HP. But it was not until November 2002 that a NetTop license was finally negotiated.

Today, HP continues to enhance NetTop to meet the needs of its customer base, including adding additional security enhancements into the technology. In addition, HP is using this experience to develop more advanced capabilities using newer technology to meet the requirements of an access cross domain solution.

While the NetTop team worked with HP to help them refine the technology, they continued to seek other commercial partners since the team believed that a competitive market would be even better for the government. After two more years of discussions with other potential partners, the team negotiated a second NetTop license with Trusted Computer Solutions (TCS). TCS was much smaller than HP but very well established in the government market for security products, and they were highly experienced at working with the security accreditation process. TCS' strengths seemed like an excellent complement to HP's for developing a significant market for NetTop.

NetTop depended upon having Mandatory Access Control (MAC) mechanisms available in a commercially supported operating system. According to Meushaw, early efforts to find commercial partners to adopt MAC were unsuccessful, so one option was to explore placing the technology into the open-source community. The research organization's strategy was to integrate MAC mechanisms into Linux modules—which later became known as SELinux. These modules were merged into the mainline kernel and released in August 2003. Eventually, the SELinux kernel migrated its way into Red Hat's Enterprise Linux product. NetTop is not only notable for its breakthrough technology, but also for the number of licenses that have been negotiated. NetTop is currently licensed by HP, Raytheon TCS, and Blue Ridge Networks.

Technology transfer with UMD—regional partner, national implications

Most technology transfers involve licensing NSA intellectual property to existing commercial companies. However, some transfers involve multistep agreements with academia that result in new start-ups. Such is the case with NSA's long-time partner—the University of Maryland, College Park (UMD). Located just 20 miles down the Route 295 corridor from Fort Meade, UMD is host to numerous NSA facilities including the Laboratory for Telecommunication Sciences and the Laboratory for Physical Sciences. But one little known fact is that NSA's Technology Transfer Office also partners with UMD's Office of Technology Commercialization (OTC), and this partnership has resulted in one particularly interesting technology start-up—FlexEl, LLC.

Powering devices on the cutting edge

With growing implementation of ultrasmall electronics and the revolution in ever-smaller form factors for computing and analytic applications, one significant bottleneck has been battery technology capable of meeting the required demands of such devices: How can power be provided when the source must be extremely small, lightweight, durable, reliable, inexpensive, safe, ideally rechargeable, and environmentally friendly? One promising solution has arisen out of the work of inventors at UMD, utilizing technology initially developed under contracts awarded by NSA and then licensed through OTC, in the form of an innovative electrochemical energy cell. This cell is designed to provide electrochemical power generation and capacitive storage in combination as a thin, flexible unit, capable of working in various applications.

This development culminated in recognition by UMD as their 2008 Invention of the Year in Physical Science, and in 2009, the start-up utilizing this technology, FlexEl, LLC, became the winner of UMD's Business Plan Competition. FlexEl was a member

FIGURE 1. FlexEl's BatteryCloth is completely flexible and bendable.

of UMD's Mtech Venture Accelerator, a selective program designed with rigorous goals and structure to promote business expertise and management for emerging companies and technological developments. Through this partnership, FlexEl was able to attract funding and support for further development and deployment of this technology. In 2010, the company was recognized as the Technology Transfer Company of the Year by the Maryland Incubator Company of the Year Awards Program.

FlexEl now focuses on continued refinement of this critical technology. In addressing some of the most pressing needs in battery capability, FlexEl is looking forward to what needs to be done to provide its product as a viable solution on the scale required, including improving capacity per unit area and ensuring manufacturability at volume. In preparing its technology for future use, FlexEl has developed three technologies tailored for different platform applications, currently in various stages of commercialization. Closest to market is a low-cost, high-capacity disposable thin film battery; next in line is a lower-capacity but rechargeable battery offering a longer lifetime; and furthest off (but perhaps with the most intriguing potential) is a battery capable of converting water from the environment into energy for activation and fueling of devices.

In addition to the battery technology that is at its foundation, FlexEl is also looking to make its mark through employing another technology based on an NSA invention—a radio frequency (RF) power harvesting circuit design. This technology provides the ability to capture and utilize energy in the form of ambient signals and transmissions from the environment. As the modern world is full of constantly radiated RF emissions, including those from cellular traffic and industrial, scientific, and medical (ISM) radio bands, developing this technology for use in the field would be a boon to reducing the physical power requirements of devices, as the operational life of electronics could be extended while significantly reducing their size. FlexEl is working as a licensing partner with UMD's OTC on improving the RF power harvesting circuit design and developing a first prototype in a joint venture between the state of Maryland and the Army as a proof of concept.

Currently the device operates as a very sensitive RF detector, with ultrasensitive applications moving toward energy harvesting as the company looks to expand and increase commercial viability of this nascent technology.

FlexEl and the future

Through the use and continued development of these technologies, built on the work of and in cooperation with NSA and UMD inventors, FlexEl has the ultimate goal of integrating them into an energy harvesting bloc capable of powering the next generation of ultrasmall electronics. The promise of FlexEl's goals is echoed by the approximately $2–3 million in funding received from entities including the state of Maryland, the Department of Homeland Security, and various companies in the private sector.

FlexEl's story illustrates how technology transfer comes full circle: The contribution of FlexEl's products, intertwined with the innovation of NSA and the UMD OTC, offers a significant return on investment for all—beyond financial terms. FlexEl's CEO believes that, as this technology matures and comes to market, there will be a significant impact through its potential application in achieving NSA's ultimate goals of national defense and national security.

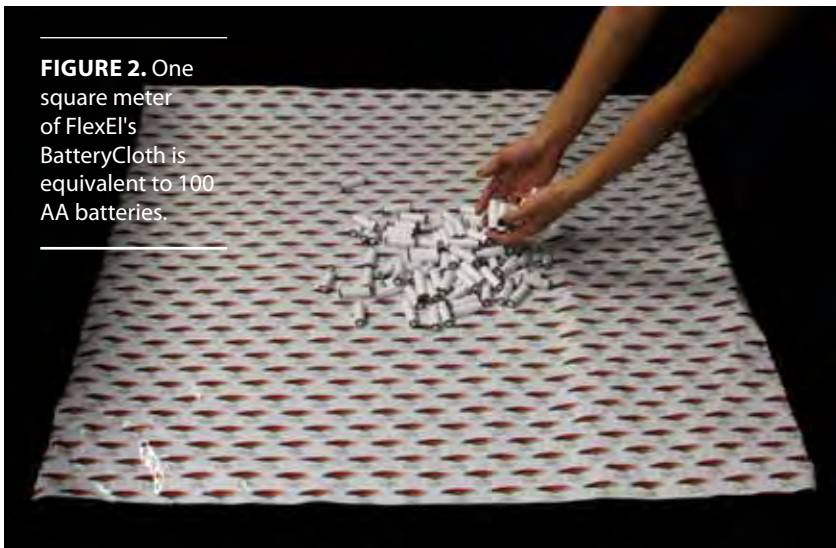


FIGURE 2. One square meter of FlexEl's BatteryCloth is equivalent to 100 AA batteries.

Bringing technology inside NSA

Carlos Salazar,
Research technology scout

Most of this issue of *The Next Wave* covers transferring technology out of NSA. But there is a flip side: Technology transfer at NSA both spins internally developed technologies out and brings externally developed technologies in. As in many scientific and technical organizations, the Research Directorate of NSA uses the tried and true method of technology scouting to uncover technological gems and bring them inside NSA. Research Directorate technology scouts focus on three key activities:

- Technology identification,
- Technology evaluation, and
- Technology outreach.

These interdependent activities are used to discover new technologies or new developments in previously mature fields that are useful for increased awareness or for direct use by an NSA program.

Technology identification requires persistent curiosity and perseverance. In the hunt for new and emerging technologies, technology scouts attend conferences, workshops, and panels. They participate in meetings and demonstrations and commission and study research surveys. Scouts can also be asked to perform a certain level of due diligence on customer requests and assess the merit of unsolicited proposals that come into NSA.

Technology evaluation involves the alignment of technologies with technical problems of interest to NSA. If a topic match exists between a technology and a technical problem, the capabilities of the technology are reviewed to determine applicability. Technology scouts must have both deep technical knowledge of a small range of subjects and more limited knowledge in a wide range of fields. Key to technology evaluation is the ability to recognize promising technologies and make estimates of the capabilities of the individuals or organizations that are proposing them. In this way, technology scouts can winnow technology opportunities so that only the most promising move forward.

Technology outreach focuses on maintaining affiliations with industry and academia and collaborating with federal government and intelligence community related groups. Technology scouts also engage with state and local organizations.

The preceding is an accurate but rather dry description of the very exciting job of technology scouting within NSA's Research Directorate. For an engineer, what is technology scouting like from day to day and week to week? It's nothing less than amazing. Technology scouts see NSA and its functions at every different level and in context of the larger intelligence community. Technology scouts constantly learn about new technologies and the latest innovations. They also meet new people from within NSA, the broader intelligence community, universities, and state and local governments. In addition, they meet with many entrepreneurs and companies, both large and small. Some of the customers are looking for brand new ideas and hitherto unnoticed scientific phenomena, while others are looking for finished or nearly finished products that can be used right away. To give you a better feel for what technology scouting is all about, the following is a first-hand account of a typical week in the life of a technology scout.

A week in the life of a technology scout

Monday

I arrive at the office, review my emails, and check my schedule for the day. Because I'll be in and out a lot this week, I need to make sure that my travel arrangements are taken care of and any outstanding tasks are covered. I prepare for a regularly scheduled meeting with a customer. He arrives at my cubicle, and I ask him about some hardware prototypes that I delivered to him a few months earlier. He has finished his evaluation of the hardware, so I collect the hardware and drop it off with another customer interested in the technology.

After lunch, I have a regular teleconference with representatives from many of the intelligence community agencies. During these teleconferences, we discuss technologies and companies and exchange feedback. After the meeting, I write up my notes on the teleconference. In the afternoon, I leave to attend another regularly scheduled meeting with a researcher. Following that meeting, I get a phone call about an outreach event sponsored by the acquisition office. They want representatives from the Technology Transfer Program and Technology Scouting to speak at an upcoming event a few months away. After checking my calendar, I reserve the time. Finally, I make some phone calls to check on the progress of ongoing technology transfers and finish up my day studying the latest innovations in software-defined radio.

Tuesday

My day starts at an industry partner location for a technology showcase. When I arrive at that facility, I recognize some retired NSA colleagues and converse with them until the session opens. *(Have to maintain those contacts!)* Soon the director for the showcase calls the meeting

to order and introduces the five companies that will be presenting. Each company has 30 minutes to introduce themselves and what they do. We have a 10-minute period between each company's presentation to discuss the capabilities presented and exchange feedback regarding the merits of presentation. Four hours fly by like nothing, and the meeting runs over the allotted time. The companies represent a range of technologies from biometric devices for security applications to visualization software and analytic algorithms. One company catches my eye. They have a patented technology that I think could be of great use to a specific customer. The company reps have some hardware at the showcase, so I take the opportunity to examine it and ask questions. Some temperature controls are involved, and I'm troubled by the lack of insulating material in the device. In the end, I decide that the company isn't a good fit for the applications I had in mind.

After the showcase, I grab lunch at a local eatery and discuss the companies with a fellow employee in attendance from NSA's Office of Small Business Programs and one of my recently retired colleagues. I then drive back to Fort Meade to meet with a company that has a web-based tool for soliciting information from companies on their research efforts. The tool manages data flow from data ingestion to final storage while supporting interactive evaluations of the research offerings. The tool looks promising but the timeline for our efforts is too long. I propose some modifications to the tool to support some of our needs and head home for the day.

Wednesday

Today I document the previous day's work and evaluate some of the unsolicited proposals forwarded from the Acquisition Office. A number of these proposals are sent in by well-meaning individuals with unique ideas. Some of the proposals are from universities with specific

research on topics of interest to NSA. Some of the proposals are from start-up companies trying to get business with NSA. The problems identified by the proposers are often relevant, but they lack the proper resources or background to deliver a viable solution. Sometimes offices are interested in a proposal but lack the funds to pursue it. Occasionally, a proposal comes in that matches a current need in an office and a contractual arrangement can be worked out. Those are the best.

After lunch, I meet with a representative of a company that attended an NSA-sponsored Business in a Minute activity. Business in a Minute is like speed dating all day, but with businesses instead of potential romantic partners. It's held locally, and different organizations from NSA have representatives there ready to hear 10-minute pitches from a steady stream of companies who want to learn more about NSA and win contracts. Every 40 minutes you get a brief break, which often isn't a break at all as company reps try to grab your attention. This particular company had some intriguing database analytics and merited a follow-up visit. I've scheduled a room at another location for the meeting since the company has no cleared employees. The technology demonstration is promising, and the ideas seem sound. I ask a number of questions and like the answers I get. The company, like most these days, has a cloud computing strategy and could be a fit with the right customer. I ask for additional information and thank them for the demonstration.

Thursday

Today I fly out to the Midwest to give a presentation at a government outreach event. Since I decided to be "fiscally responsible" and not rent a GPS from the rental car company, I have to rely on my Google Maps printout to navigate to the hotel. Even though the roads have changed a bit from my printout, I eventually get there. At the speaker's reception that evening, I find myself next

to an Air Force brigadier general in uniform and several company and university representatives. I strike up a conversation with a NASA engineer whose talk concerns green power initiatives. We talk about flywheel storage and he informs me that NASA is actually doing a technology transfer of flywheel storage technology that lasts much longer than current commercial technology. Later in the evening his ride leaves without him, and I end up driving him back to the hotel. Having a navigator at night in a strange city is a relief after my earlier adventures getting to the conference.

Friday

The outreach event presentations begin this morning. I transfer my PowerPoint files to the display laptop and run through them to make sure all is in order. The morning talks are divided up into two different sessions. My newfound NASA friend is speaking in the other session, so I can't listen to his presentation. I'm scheduled to speak after lunch in a combined session. The speaker prior to me runs over time—by a lot. The event organizers quietly ask if I can cut down my presentation. I answer "yes" and mentally toss out half my slide deck. Following my presentation, there is a round table with the government representatives answering questions from the many businesses' attendees.

After that, the outreach event ends, but my day's not over. I'd previously agreed to meet with a company representative seeking to do business with NSA. I can't actually talk with her yet because quite a few people want to talk with me about NSA contracting and give me business pitches and cards. After politely responding to their inquiries, I finally meet with the company rep with whom I'd actually scheduled time. We pick a quiet place in the lobby next to the Internet terminals so that she can run her demo showing different levels of the product. It's an interesting technology, but the demo is really getting drawn out. The event organizer takes pity on me and

asks if I want to go out to dinner with him and a former marine now working for the Marine Corps as a civilian. I gratefully accept, and the demo wraps up.

Saturday

Go to Brian's soccer game.

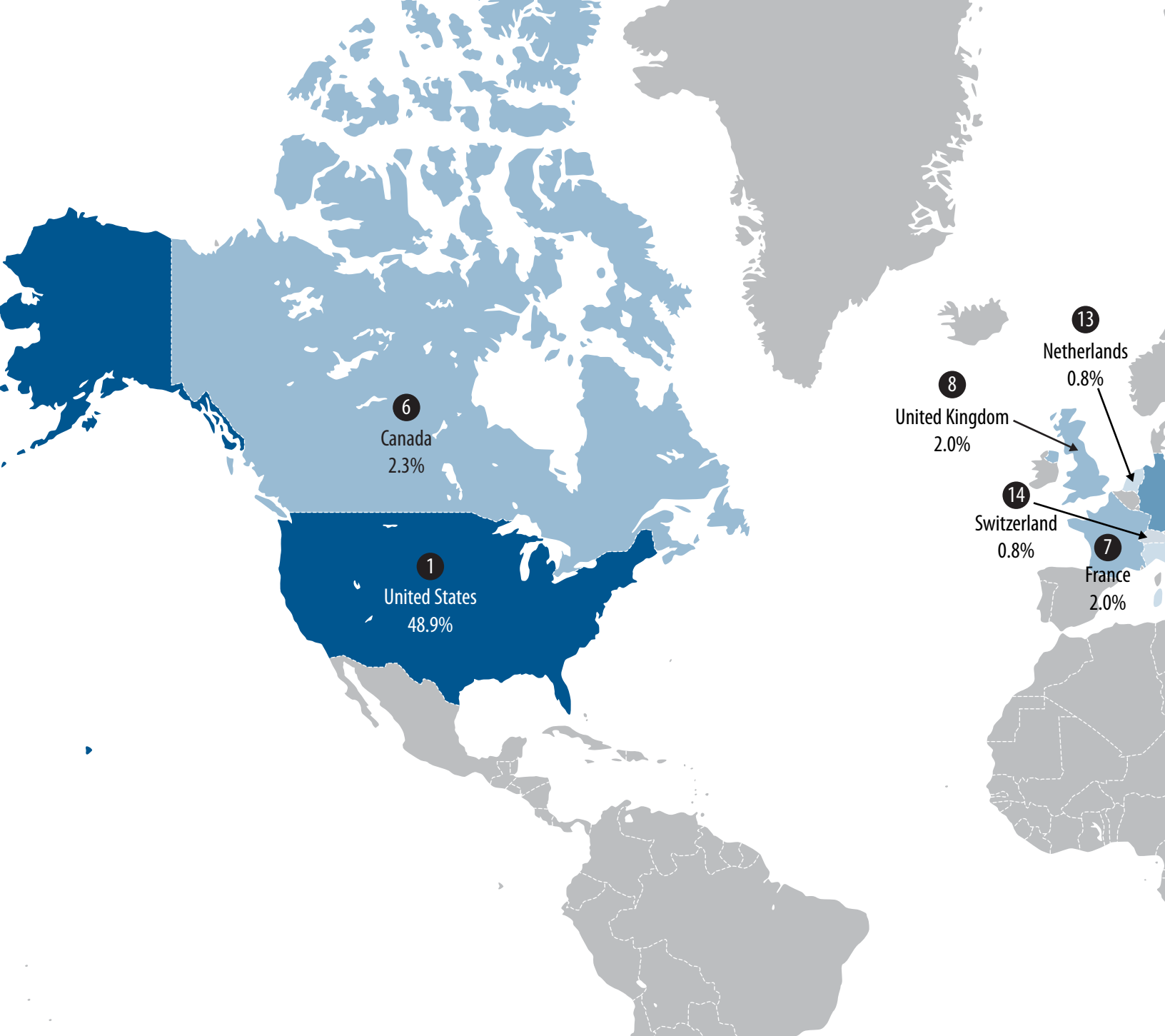
Su

Co

The previous events are all abstracted from the typical week of a technology scout. Technology scouts constantly learn new and exciting things, meet new people, travel, and, of course, document their findings. Good relations with NSA technical leaders are essential to understanding the true needs of the different organizations. In the end, a successful NSA technology scout has to forge and maintain an ever-widening network of human contacts and sources so that the right people get the right technology at the right time. You never know when, where, or how the next technological gem will appear.

Tuesday

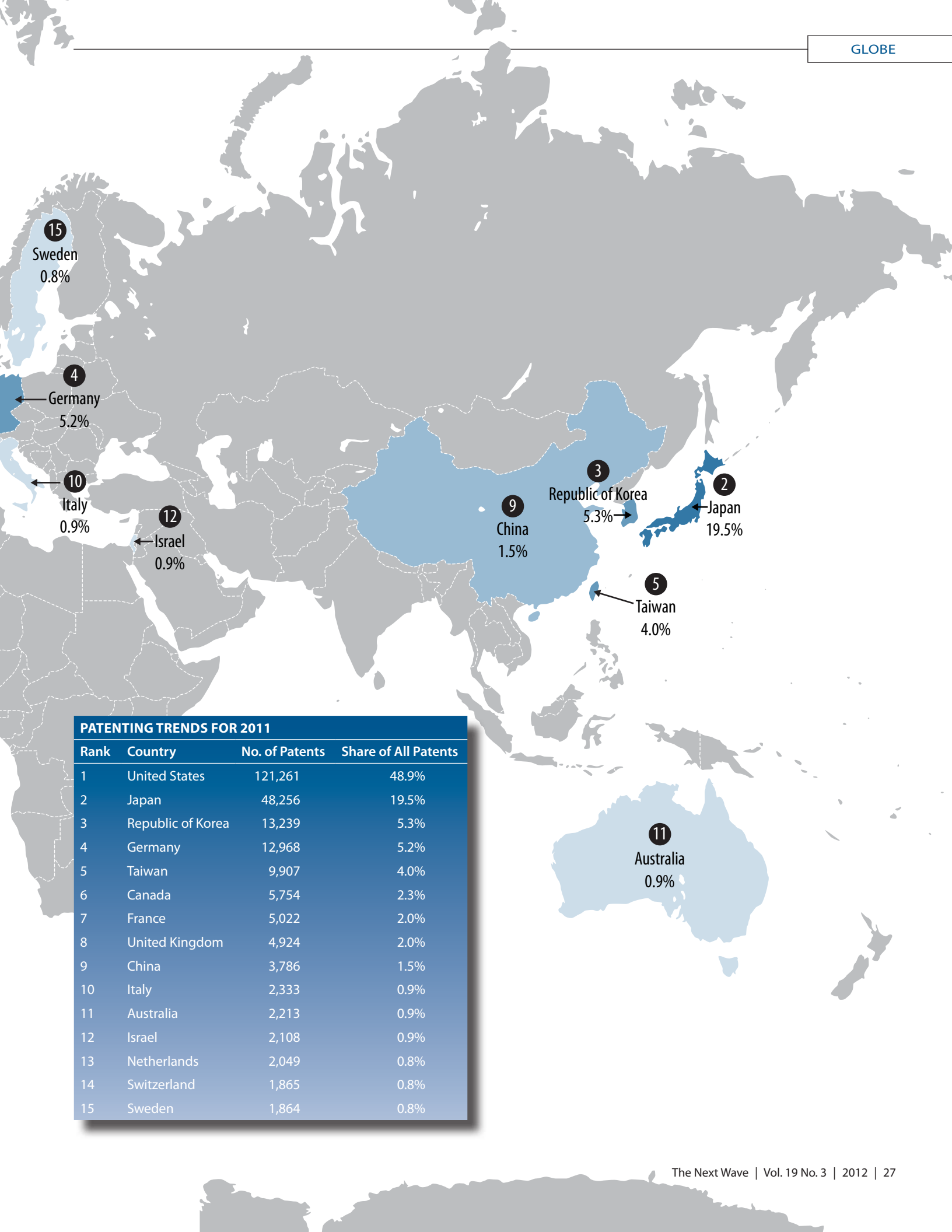
Vacation with the family!



GLOBE AT A GLANCE

Patenting trends for 2011

This map shows the 15 countries that received the most US patents during 2011. Patent origin is based on the residence of the first-named inventor. The totals include utility, design, plant, and reissue patents, and statutory invention registrations. This data, provided by the United States Patent and Trademark Office, is available at www.uspto.gov/web/offices/ac/ido/oeip/taf/pat_tr11.htm.



PATENTING TRENDS FOR 2011

Rank	Country	No. of Patents	Share of All Patents
1	United States	121,261	48.9%
2	Japan	48,256	19.5%
3	Republic of Korea	13,239	5.3%
4	Germany	12,968	5.2%
5	Taiwan	9,907	4.0%
6	Canada	5,754	2.3%
7	France	5,022	2.0%
8	United Kingdom	4,924	2.0%
9	China	3,786	1.5%
10	Italy	2,333	0.9%
11	Australia	2,213	0.9%
12	Israel	2,108	0.9%
13	Netherlands	2,049	0.8%
14	Switzerland	1,865	0.8%
15	Sweden	1,864	0.8%

ACCORDING TO THE EXPERTS

Growing demand for intellectual property changes the face of innovation[a]

The World Intellectual Property Organziation (WIPO), the United Nations agency dedicated to the use of intellectual property (IP) as a means of stimulating innovation and creativity, published their 2011 report, "The changing face of innovation."[b] With global demand for patents rising from 800,000 applications in the early 1980s to 1.8 million in 2009, the report concludes that growing investments in innovation and the globalization of economic activities are key drivers of this trend. As a result, IP policy has moved to the forefront of innovation policy. The report points to a number of implications of the growing demand for IP rights, namely:

- Knowledge markets based on IP rights are on the rise. Evidence suggests that firms trade and license IP rights more frequently. Internationally, royalty and licensing fee revenue increased from $2.8 billion in 1970 to $27 billion in 1990, and to approximately $180 billion in 2009—outpacing growth in global gross domestic product (GDP). New market intermediaries have emerged, such as IP clearinghouses and brokerages.

  Evidence shows that knowledge markets enable firms to specialize, allowing them to be more innovative and efficient at the same time. In addition, they allow firms to control which knowledge to guard and which to share so as to maximize learning—a key element of modern open innovation strategies.

- Patenting has grown especially fast for so-called complex technologies—that is, technologies consisting of many separately patentable inventions where patent ownership is often widespread. This partly reflects technological change. For example, complex technologies include most information and communications technologies that have seen rapid advances over the past decades.

  At the same time, some complex technology industries—notably, telecommunications, software, audiovisual technology, optics and, more recently, smartphones and tablet computers—have seen firms strategically build up large patent portfolios. As a result, there is concern that increasingly dense webs of overlapping patent rights slow cumulative innovation processes. Collaborative approaches, such as patent pools, can to some extent address such concerns; however, making sure that crowded patent landscapes do not hold back innovation and entrepreneurship demands careful attention by policymakers.

- In this regard, well-functioning patent institutions have become a cornerstone of successful innovation systems. They perform the essential tasks of ensuring the quality of patents granted and providing balanced dispute resolution. Unprecedented levels of patenting have put these institutions under considerable pressure. Many patent offices have seen growing backlogs of pending applications. In 2010, the number of unprocessed applications worldwide stood at 5.17 million. The choices patent offices make can have far-reaching consequences on incentives to innovate.

- Many countries have put in place policies to harness public research for innovation. One element of such policies is to incentivize patenting by university and public research organizations (PROs) and the subsequent commercial development of their inventions. Accordingly, there has been a marked increase in patent applications by these organizations. University and PRO filings under the WIPO's Patent Cooperation Treaty (PCT) have grown from close to zero in the 1980s to more than 15,000 in 2010. High-income economies account for most of this growth—notably France, Germany,

a. This content comes from WIPO's November 14, 2011 press release, available at www.wipo.int/pressroom/en/articles/2011/article_0027.html.
b. The full report is available at www.wipo.int/econ_stat/en/economics/wipr/.

Innovation growth is no longer the prerogative of high-income countries alone; the technological gap between richer and poorer countries is narrowing. Incremental and more local forms of innovation contribute to economic and social development, on a par with world-class technological innovations.

WIPO Director General Francis Gurry

Japan, the UK, and the US. However, many middle income countries have also seen marked growth. In the case of universities, China leads with 2,348 PCT filings from 1980 to 2010, followed by Brazil, India, and South Africa. In the case of PROs, China and India alone represent 78 percent of total fillings from middle-income countries.

Policy reforms aimed at promoting patent-based university technology transfer have multifaceted effects on research institutions, firms, the science system, and the economy.

Other conclusions of the report include:

- While high-income countries still dominate global research and development (R&D) spending, the geography of innovation has shifted. Global R&D expenditures almost doubled in real terms from 1993 to 2009. Most R&D spending still takes place in high-income countries—around 70 percent of the world total. They spend around 2.5 percent of their GDP on R&D, more than double the rate of middle-income economies. Low- and middle-income economies have increased their share of global R&D expenditure by 13 percentage points between 1993 and 2009. China accounts for most of this increase—more than 10 percentage points—propelling China to the world's second largest R&D spender in 2009.
- Data on broader investment in intangible assets are only available for selected high income countries. They show that such investment has grown rapidly; in a number of countries, firms now invest more in intangible than in tangible assets. In Europe, investment in intangibles amount to as much as 9.1 percent of GDP in Sweden and the UK.
- There is clear evidence that innovation is increasingly international with a sharp increase in the share of peer-reviewed science and engineering articles with international coauthorship and a rising share of patents which list inventors from more than one country. In addition, multinational firms more and more locate their R&D facilities in a variety of countries—with certain middle-income economies seeing particularly fast growth. The rising share of middle-income countries in the global economy, in turn, is reorienting innovation towards the demands of those countries.
- Some evidence exists that innovation has become more collaborative and open, but assessing the true scale and importance of new approaches is challenging. For one, it is difficult to draw a clear distinction between open innovation strategies and long-standing collaborative practices, such as joint R&D, joint marketing or strategic partnerships. For another, certain elements of open innovation strategies—such as new policies internal to firms or informal knowledge exchanges—cannot easily be traced.
- Notwithstanding this uncertainty, collaboration in the innovation process can benefit firms and society. Joint IP production occurs through R&D alliances, in particular contractual partnerships and equity-based joint ventures. Data on such alliances are limited and sometimes difficult to interpret, but they suggest that firms in the ICT, biotechnology, and chemical industries most frequently enter into such alliances. Society usually benefits from such collaboration as it enhances the efficiency and effectiveness of the innovation process.

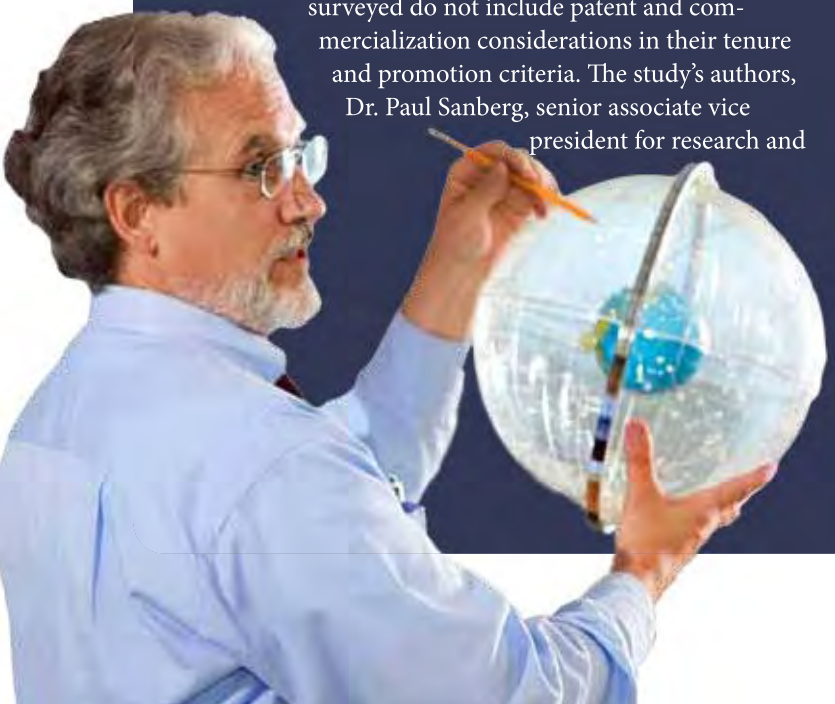
POINTERS

Patent protection may hinder innovation

Results of a study suggest that, contrary to popular belief, greater amounts of innovation, productivity, and social utility may occur when people are required to pay damages for illegally using an invention rather than when they are prohibited from using it at all. Researchers Bill Tomlinson, informatics professor at the University of California, Irvine, and Andrew Torrance, professor at the University of Kansas School of Law, conducted a study providing experimental evidence that the most innovation may result when inventors receive no protection from the legal system. Using the "Patent Game," an interactive computer-based model that attempts to simulate patent systems, Tomlinson and Torrance conducted controlled experiments to evaluate the merits of property rules (which expressly prohibit people from utilizing a patent owner's invention) and liability rules (which require infringers to pay damages but do not bar them from using an invention). "Conventional wisdom says people will invent less if property rights are not strongly enforced," Torrance said. "However, we found that the threat of prohibition actually dampened innovation." Their paper, "Property rules, liability rules, and patents: One experimental view of the cathedral," appears in the 2012 spring issue of the *Yale Journal of Law & Technology.*

Should patents and commercialization activities count toward faculty tenure and promotion?

Increasingly, universities are including faculty member patents and commercialization activities in deciding tenure and promotion. However, a small study conducted in 2011 revealed that 75 percent of North American universities surveyed do not include patent and commercialization considerations in their tenure and promotion criteria. The study's authors, Dr. Paul Sanberg, senior associate vice president for research and innovation at the University of South Florida and president of the National Academy of Inventors, Ginger Johnson of *Technology and Innovation,* and Dr. Ashley Stevens, former senior research associate at the Boston University School of Management and past president of the Association of University Technology Managers, found that the universities that take patenting and commercialization into account share additional features: They are public institutions, they consider US patents a priority, they have adopted the policy in the last six years, and they publish their tenure and promotion guidelines. The authors note that adding patent and commercialization activities to tenure and promotion criteria will encourage young professors to innovate early, which will in turn boost universities' research budgets. They point out that in 2009 universities earned about $1.8 billion in royalties from academic inventions, an increase over $1.6 billion in 2008 and $1.3 billion in 2007. The report, "The role of patents and commercialization in the tenure and promotion process," appears in *Technology and Innovation, Proceedings of the National Academy of Inventors* (Vol. 3, No. 3).



Background on the America Invents Act, from the US House of Representatives Committee on the Judiciary

On September 16, President Obama signed into law the *Leahy-Smith America Invents Act* (H.R. 1249), a bipartisan, bicameral bill that updates our patent system to encourage innovation, job creation, and economic growth. Both Houses of Congress overwhelmingly supported the proposal, which was sponsored by House Judiciary Committee Chairman Lamar Smith (R-Texas). The House of Representatives passed H.R. 1249 by a vote of 304-117 earlier this year. The Senate passed the bill by a vote of 89-9. Senator Patrick Leahy (D-Vermont) partnered with Chairman Smith on the legislation. Congressman Smith led the House efforts on patent reform for more than six years.

Much-needed reforms to our patent system are long overdue. The last major patent reform was nearly 60 years ago. Since then, US innovators have developed cell phones and launched the Internet. And yet the laws protecting the technologies of today are stuck in the past.

Our outdated patent system has been a barrier to innovation, unnecessarily delaying American inventors from marketing new products and creating jobs for American workers. It takes over three years to get a patent approved in the US. American innovators are forced to wait years before they can hire workers and market their inventions. Meanwhile, our competitors are busy developing new products that expand their businesses and grow their economies. This year, for the first time, China is expected to become the world's number one patent publisher, surpassing the US and Japan in the total and basic number of patents. We cannot expect America's innovators and job creators to keep pace with the global marketplace with the patent

system of the past. We need a system that ensures patent certainty, approves good patents quickly, and weeds out bad patents effectively.

The *Leahy-Smith America Invents Act* is one of the most significant job creation bills enacted by Congress this year. The Act implements a first-inventor-to-file standard for patent approval, creates a postgrant review system to weed out bad patents, and helps the Patent and Trademark Office address the backlog of patent applications. The enactment of H.R. 1249 is a victory for America's innovators and job creators who rely on our patent system to develop new products and grow their businesses. The *America Invents Act* brings our patent system into the 21st century, reducing frivolous litigation while creating a more efficient process for the approval of patents. These reforms will help the innovators and job creators of today launch the products and businesses of tomorrow.

Software companies ignore patent infringement

In an article to be published in *New York University Annual Survey of American Law,* Christina Mulligan and Timothy Lee assert that patent litigation is rampant throughout the software industry because the cost for a company to figure out if they are infringing upon a patent (i.e., discovery costs) is prohibitively high. They point out that discovery costs are high because of the sheer number of software patents and their disorganization. Software products contain thousands of lines of code, any of which may be patentable. Raising a popup window to update software, the slide-to-unlock feature on an iPhone, and the one-click purchasing feature on a retailer's website—they are all patented. Mulligan and Lee argue that information collected about software patents is not standardized and, thus, not indexable. Their article, "Scaling the patent system," claims that thoroughly clearing a single software product from patent infringement would require more patent attorneys than exist in the US and would cost more than the entire value of the software industry. As a result, many software companies do not try to avoid patent infringement. To remedy this problem, Mulligan and Lee suggest patent policy reform, such as excluding industries with high discovery costs from patent protection, establishing an independent invention defense, or eliminating injunctions.

Printing intellectual property in 3-D

In January 2012, The Pirate Bay, a controversial file-sharing website, launched a new category of downloads termed, "physibles"—digital design files that can be printed as physical objects from a 3-D printer. 3-D printers work by building up an object one layer at a time. Currently, they are used in industrial settings to create objects such as artificial jaws and airplane components, but personal 3-D printers are on the horizon. 3-D printers will allow the general public to legally create objects for use and/or sale that they may have otherwise purchased because, unlike text, music, and video, which are protected by copyright immediately upon creation, the majority of physical objects are not protected by an intellectual property right. Intellectual property rights for physical objects and designs come in the form of patents and trademarks, and they are harder and more expensive to obtain than a copyright. Additionally, file-sharing websites like The Pirate Bay may open the way for people to use 3-D printers to illegally reproduce patented physical objects. Just as the entertainment industry responded to illegal file-sharing with digital rights management techniques that prevented a file from playing on an unauthorized device, manufacturers of physical objects may respond to 3-D printers by developing techniques to protect digital design files. (Photo depicts a necklace, created by Dutch jewelry designer and conceptual artist Ted Noten, made of glass fiber-filled nylon printed from a 3-D printer.)

ipAwarenessAssessment Beta

A business and inventors IP education tool

uspto NIST

Assessing intellectual property awareness

The US Department of Commerce's Patent and Trademark Office (USPTO) and National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP) unveiled the web-based Intellectual Property Awareness Assessment Tool on March 30, 2012. The tool is designed to help manufacturers, small businesses, entrepreneurs, and independent inventors easily assess their knowledge of intellectual property (IP).

"Understanding and protecting IP is an important part of the process of bringing innovations to the marketplace," said Under Secretary of Commerce for Standards and Technology and NIST Director Patrick Gallagher. "We hope this new tool will be useful for companies and individuals helping them to create value and be more globally competitive."

Intellectual property is a key concern of small businesses owners, who can secure significant competitive advantages by exercising the rights they hold to their innovations. However, many individuals are often unaware of their rights and miss the opportunities they can provide. USPTO and NIST MEP developed the IP Awareness Assessment Tool as a way to help educate innovators about these rights.

The tool enables users to measure and increase their awareness of IP issues, relevant to their creative projects and business goals. Users answer a comprehensive set of questions regarding IP, after which the tool provides a set of training resources tailored to specifically identified needs. The tool is available on USPTO's website at www.uspto.gov/inventors/assessment.

SPINOUTS

News from the Technology Transfer Program

It is only fitting that this inaugural column from NSA's Technology Transfer Program (TTP) appears in an edition of *The Next Wave* focusing on intellectual property and technology transfer. Within this space, the TTP will be bringing you interesting and informative topics within technology transfer, intellectual property marketing, and new patents, as well as transfer success stories. For our first column, we will be discussing Technology Readiness Levels, or TRLs.

Technology Readiness Levels (TRLs) are a scale used by industry and government to determine the maturity of technologies to be incorporated into another type of system. In NSA's TTP, TRLs are used informally when evaluating technologies for transfer. Generally, the higher the TRL, the more likely the technology will successfully transfer to a commercial environment.

Although TRLs were originally conceived at NASA in the 1970's, similar but different definitions are now used by various agencies, including the US Department of Defense (DoD). The following definitions are taken from the DoD 2011 Technology Readiness Assessment Guidance, prepared by the Assistant Secretary of Defense for Research and Engineering.

- **TRL 1. Basic principles observed and reported.** This is the lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
- **TRL 2. Technology concept or application formulated.** Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
- **TRL 3. Analytical and experimental critical function and/or characteristic proof of concept.** Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
- **TRL 4. Component validation in a laboratory environment.** Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared with the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
- **TRL 5. Component validation in a relevant environment.** Fidelity of technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components.
- **TRL 6. System/subsystem model or prototype demonstration in a relevant environment.** Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. This level represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.
- **TRL 7. System prototype demonstration in an operational environment.** Prototype near or at planned operational system. This level represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, in a vehicle, or in space).
- **TRL 8. Actual system completed and qualified through test and demonstration.** Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
- **TRL 9. Actual system proven through successful mission operations.** Actual application of the technology in its final form and under mission conditions takes place, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

iN054744