POLICING THE DIGITAL ENVIRONMENT

Toby M. Finnie

The Wild, Wild West: Part I

The development of telegraphs and networks is significant for understanding the Internet because it demonstrates the relentless push toward more speed, more capacity, more raw volume, more "consumers."

— Anne B. Keating[i]

I sat at my desk, glumly mulling over an assignment. With a deadline looming, an analysis discussing the near and far future of Internet crime's impact on the department seemed no nearer completion than it was a month ago when Assistant Chief Murphy assigned it to me.

Strategic planning? It was difficult to grasp how cybercrime might affect us next month, let alone twenty years from now! I couldn't seem to draw a bead on it. Every week there seemed to be a new techno-toy, or news of a new computer crime scheme. If the bad guys weren't hacking they were phreaking, pharming and phishing.[5] I felt as if I was trying to grab smoke!

I glanced heavenward and silently thanked Hiram B. Thomas, my 92-year-old grandfather, for a temporary reprieve. When I'd spoken to him a week before he died, I'd griped about the cybercrime report. There was nothing, I grumbled, that could compare to the impact cybercrime was having on law enforcement.

If I was looking for sympathy (and I was) I didn't get it from Granddad.

"Your grandma used to say 'There's nothing new under the sun!'" Granddad had replied, "You're a smart boy. You'll figure it out."

The temporary reprieve arrived in the form of a small package mailed by the Executor of Granddad's estate. My grandfather had died before he could deliver it to the post office.

Curious, I opened the package. A note, written in my grandfather's shaky, not quite indecipherable hand was wrapped around an old leather-bound journal. It read:

> "This belonged to Anna Parker Thomas, my great grandmother. She was born in Chambersburg, PA in 1846. When Civil War recruitment depleted the local work force — and took away the eligible young bachelors, Anna hired on as a messenger with the Adams Express Company in 1862. She promoted to telegrapher a couple of years later.6 I think you will find her journal useful

[5] "Phreaking" involves theft of telecommunication services. "Phishing" attempts to capture personal information by prompting users to visit a fake website. "Pharming" redirects a user to a fake website without the user being aware of the redirection.

[6] Many believe that women first entered the telecommunications industry as telephone operators, to replace the unruly boys who were employed to operate switchboards. However, when the telephone was first publicly demonstrated, in 1876, women had already been part of telecommunications technology for thirty years — as telegraph operators and managers. *See* Schlereth, Thomas J. (1991) *Victorian America: Transformations in Everyday Life 1876-1915* (New York: Harpers Collins 1991) p 4

as you prepare to write your report. Remember, there is nothing new under the sun! — Granddad."

I spent the next hour skimming through Anna's journal. Covering 25 years of telegraph, railroad and personal history, her entries wove a fascinating tale of her life and times working for the Wild, Wild West's first version of the Internet: the telegraph.

The Pacific Telegraph Act of 1860[7] called for the facilitation of communication and a year later, Western Union networked with several other telegraph companies to link the east and west coasts of the United States. Six years later, a transatlantic telegraph cable connected the United States with Europe.

In May 1869, Union Pacific and Central Pacific conjoined tracks to become the first transcontinental railroad, opening the western territories to expansion. Following along railroad rights of way, telegraph wires crisscrossed the country, awed the public, and forever changed the conduct of business.

That the public was enthralled by the rapid transmission of dash-dot encoded messages was an understatement, in light of the fact that mail sent from St. Louis, Missouri to Sacramento, California via Pony Express took 11 days.[ii]

The "email" of its day, a telegraph message could be encoded and transmitted from San Francisco to New York in under fifteen minutes. Even more noteworthy, the same message could be transmitted to thousands of recipients, paving the way for snake oil salesmen to mass-market worthless products.[iii]

Two days after the intercontinental telegraph was completed the Pony Express became obsolete and hung up its saddles forever. Other businesses flourished.

Richard Sears, a telegraph operator and railroad station manager, started a mail order service to sell watches via the telegraph. His business developed into what would later be known as the Sears-Roebuck Company. All manner of goods could be ordered by telegraph and shipped by express companies: even mail-order brides![8] Thomas Edison introduced the stock ticker and printing telegraph. In Europe, the Associated Press formed an alliance of Morse telegraph services and transmitted news dispatches worldwide.

Relationships and romances heated up the telegraph wires.[iv] Alexander Graham Bell was even said to have complained about "unseemly" messages exchanged between telegraph operators. Telegraphers developed their

[7] The Pacific Railway Act, July 1, 1862. *An Act to aid in the Construction of a Railroad and Telegraph Line from the Missouri River to the Pacific Ocean.* (U. S. Statutes at Large, Vol. XII, p. 489 ff.)

[8] In addition to a regular money order service, the telegraph companies maintained a telegraphic shopping service, permitting the purchase by telegraph of any standardized article that could be picked up or delivered by parcel post or express. SEE *Ross, Nelson E. How To Write Telegrams Properly.* 1928 *http://www.telegraph-office.com//pages/telegram.html#How%20to%20Save*

own jargon in Morse code and when business was slow, they played games with other telegraph operators.

> For amusement at such lonely stations, two telegraph operators, maybe 75 miles apart, would both plug into the same “spare telegraph wire circuit” and play games by wire such as chess or checkers or certain playing-card games, or maybe just to “chew the rag” or listen in on Western Union and get the latest news even before it came out in the city newspapers.[v]

The telegraph further extended its reach in May 1897 when Guglielmo Marconi transmitted the first wireless telegraph communication over water.

Expanding railroads, telegraph and express delivery companies set up agencies in the territorial West so their businesses could be managed remotely. Entrepreneurs, cattlemen and homesteaders settled near the agencies. As a consequence, communities rapidly developed where buffalo formerly roamed.

The U.S. Post Office took advantage of the rail systems, shipping huge volumes of mail across the country, even sorting mail while in transit. Express companies delivered commodities and transported gold, securities and cash via rail car. Commerce was on the move and following the money, so were the criminals:

> By the very nature of their physical construction, railroads became the prime prey of many well-organized bands of outlaws. Theft was rampant and the losses in dollars of freight, parcels and luggage were overwhelming to the railroad companies. Bridges, tunnels, stations, tracks and railroad cars were dynamited in daring holdups. Following the Civil War, thousands of unemployed soldiers/hobos took to the rail yards and to the rails to loot and rob.[vi]

Just as flim flam artists promoted bogus lotteries and other get rich quick schemes via the telegraph, opportunistic outlaws also took advantage of new technologies. They rode fast horses, used high-powered rifles and smokeless powder (so they could fire at pursuers from a distance without giving themselves away). They hired safecrackers to help them break into safes and employed explosives experts to blow up railroad tracks and trestles.

Family members and gullible young men looking for excitement were recruited to join outlaw gangs. In Highwaymen of the Railroad,” William Pinkerton wrote:

> “The majority of these robbers are recruited from among the grown boys or young men of small country towns. They start in as amateurs under an experienced leader. They become infatuated with the work and never give it up until arrested or killed.”[vii]

Outlaw gang members wore disguises and used aliases — “Kid Curry” (aka Harry Logan), “Tall Texan” (aka Ben Kilpatrick) and the “Sundance Kid” (aka Harry Longbaugh) were but a few — to mask their identities.

They were enticed by large sums of money and showed little fear of arrest for their meticulously planned and well-executed robberies. They hacked into telegraph systems to monitor law enforcement activities and cut telegraph wires to impede police operations.

Unlike romanticized, movie-inspired portrayals of outlaws leaping from horseback onto moving railcars, robbers gained access by laying in wait and attacking when trains stopped at refueling stations. Sometimes railroad tracks were dynamited or trestles were burned, with resulting injuries and death to passengers and crewmen when train cars derailed. Gawking passengers, curious to see why their train was "held up," were sometimes shot for their inquisitiveness.

To avoid arrest, some gangs split up and escaped across state lines or territorial and international borders. Others retreated to remote hideouts. Some gangs (the James Brothers, for example) made no effort to hide; so confident were they of community protection.

Federal response was lethargic. The U.S. Army had jurisdiction over the territories but the army was no good at policing and already had its hands full dealing with Indian Wars. U.S. Marshals also had jurisdiction but were very thinly spread, out-manned and out-gunned. They were often forced to deputize posses or seek assistance from citizen vigilance committees. Some frontier towns were lawless and dangerous. The outlaws "became terrors to the community in which they lived. It was impossible to get the necessary evidence to convict them, as, to a certain extent, they controlled, through terrorizing, some of the local judges; and the local authorities, either through sympathy or fear, were afraid to do their duty."[viii]

Local law enforcement (where there was local law enforcement) was overwhelmed. Police had expanding responsibilities, limited operating funds, and poorly trained personnel. Only the larger police agencies could afford to keep up with technology. The smaller agencies were forced to make do with what they had—and what they had wasn't much. Federal criminal statutes were all but nonexistent; state statutes were inadequate.

Even so, police worked with the tools they had. They printed and distributed wanted posters and shared information with neighboring law enforcement agencies via telegraph. To help maintain law and order, they deputized citizen posses and sought the assistance of private sector investigators. (Unknown in local communities, private investigators could more easily conduct covert investigations, especially in situations where the outlaws controlled the citizenry.)

The railroad and express companies, needing to protect assets, fought back. They pressured politicians to enact statutes such as the Pennsylvania Railroad Police Act (1865)[9] and the

[9] On February 27, 1865, the Pennsylvania legislature enacted the Railroad Police Act — the first act officially establishing railroad police. The act authorized the governor of the state to appoint railroad police officers, and gave statewide authority to these officers. This act provided the model legislation for the other states to follow. Norfolk Southern Police Department. *History of Railway Police.*

federal Mail Fraud Act of 1872 — the country's oldest consumer protection statute.[10] They lobbied Congress to make train robbing a capital offense.

Railroad companies started up their own police departments and lured experienced police investigators away from public service with offers of higher salaries.

To protect shipments and property, express companies hired guards and armed them with high-powered weapons. They reinforced strongboxes with iron stropping and bolted them to coach and railcar floorboards. They purchased heavy-duty safes and limited employee access to the combination lock codes. They contracted private detectives to relentlessly hunt down perpetrators.

A standout agency of its time was the Pinkerton National Detective Agency.[11] After enjoying a brief stint as a detective with Chicago Police Department, Allan Pinkerton started up the agency in 1851. The "Pinks" were highly successful in solving train and express company robberies, in no small part due to guiding principles and innovative investigative techniques developed by Pinkerton himself.

Pinkerton demanded the utmost integrity from his operatives and instilled in them a strict code of ethics. He hand-picked agents for their intelligence, perceptiveness and courage and in 1856 hired the first female detective in the U.S. — forty years would pass before police departments began to hire women — and Kate Warne would become one of his most successful operatives.

Working with technologists, telegraphers, and firearms experts, Pinkerton strove to ensure that his agents had up-to-date training, the newest equipment and the finest investigative tools. His agents participated in crime dramatizations and role-playing exercises, learned to wear disguises and assume various personas.

The Pinkertons incorporated science and technology in ways that presaged and shaped the future of public sector crime fighting, including crime analysis and crime mapping:

> So frequent and routine were the Gentleman Bandit's stagecoach holdups over the years that the Pinkertons had been able to plot his movements on a map of the American West.[ix]

By the 1870s Allan Pinkerton, together with his sons William and Robert, had compiled the largest collection of mug shots and criminal profile data in the world.[x] Pinkerton agents in the field gathered information about criminals from police, informants, and especially from newspaper articles.

<http://nspolice.com/history4.htm. Assessed June 1, 2007.

[10] Enacted June 8, 1872, ch. 335, § 301, 17 Stat. 283 (codified at 18 U.S.C. 63 § 1341), the mail fraud statute was one section in a recodification of the Postal Act.

[11] So profitable was Allan Pinkerton's business model that the Pinkerton National Detective Agency has been in continuous operation for one hundred and fifty-six years. Securitas AB, a Swedish company, acquired *Pinkerton* & Burns Security Services (formerly Pinkerton National Detective Agency) in July 2003. Securitas is one of the largest security companies in the world.

The information was then telegraphed to the main office in Chicago. When warranted, mug shots[12] and criminal profile data was relayed to Pinkerton and police investigators. [13]

The crime data was also used in reward posters and information bulletins such as Pinkerton's Criminal Mug Shot & Information Book that was provided to members of the American Bankers Association. That book listed photos, descriptions and general information, including handwriting samples, about 300 known criminals and described criminal "methods of forgers, sneak thieves, robbers and swindlers." It also provided tips to banks on entrapping criminals before calling the police.[14]

Pinkerton was a founding member of an organization that became known as the International Association of Chiefs of Police (IACP). As a director on the IACP board Pinkerton's vision for a centralized bureau to collect, store and maintain criminal data became a reality in 1897 with the creation of the National Bureau of Criminal Identification. In 1924, the records were permanently transferred to the Federal Bureau of Investigation.

The Pinkertons also developed a secure method for sharing sensitive information via telegraph through the use of cipher text. Copies of the cipher code were distributed to the American Bankers Association and other clients.[15]

Pinkerton agents' pursuit of suspects was relentless, even across international borders. Agents hounded outlaws Butch Cassidy and the Sundance Kid in Argentina. Dogged pursuit of the Reno Brothers after they fled to Toronto, Canada led to extradition agreement revisions between the two governments.

Pinkerton and his sons educated the business community, offering "advice and preventative measures to banks,

[12] Invented and in use by 1851, the Pantelegraph, an electrochemical telegraph, was able to transmit graphic images so that "together with the proclamation for somebody's arrest it can also provide a portrait of the criminal." Castella, Bjarne (n.d.) *The Predecessor of the Facsimile from the Last Century* (Post & Tele Museum, Denmark) <http://www.teponia.dk/museumsposten/index.php?artikelid=157> Accessed March 23, 2007

[13] Of the 195 criminal investigations binders, two-thirds cover the period of Pinkerton's greatest activity in criminal work, from 1880 to 1910. The binders contain photographs and sketches of criminals, suspects and gang members, as well as Pinkerton operatives; photographs and illustrations of burglar tools, safe-cracking equipment, and crimes in progress; "Reward" and "Wanted" posters and handbills; many press clippings from 1870 to 1938; penciled daily draft reports from detectives; criminal histories (Pinkerton "rap sheets"), gang histories, and crime chronologies. Also included are "office narratives," written by clerks, covering all or parts of an investigation; interoffice communications concerning investigations; correspondence with local law enforcement officials; correspondence with Pinkerton informants; letters to Pinkerton from criminals; and correspondence between criminals. SEE Urschel, Donna (2000) *The First Private Eye: Library Receives Pinkerton Archives*. The Library of Congress: Information Bulletin 2000) http://www.loc.gov/loc/lcib/0006/pink.html> Accessed May, 2007

[14] Samples of Pinkerton's Mug shot books can be viewed at this link: <http://www.pimall.com/nais/pivintage/pcriminalphotobook.html>

[15] Samples of wanted posters and information flyers can be viewed at this link: <http://www.pimall.com/nais/pivintage/telegraphcipher.html>

shipping offices, mail services and other enterprises that dealt with the handling and movement of money."[xi]

Nearly sixty years transpired between the first train robbery in 1866 and the last recorded hold-up in 1924. A concerted partnership effort by police, business owners, private investigators, legislators and ordinary citizens finally put a halt to the "hold ups."

I had been born into the generation of grade school students who enjoyed the smell of freshly mimeographed papers. I learned to type on manual typewriters. I didn't know much about the history and development of digital technologies that emerged in the '90s, but Granddad's axiom that "there is nothing new under the sun" resonated deeply.

As Granddad had implied I would, I was beginning to see the analogous relationship between the technological challenges faced by 19th Century detectives and 21st Century cybercrime investigators.

The Wild, Wild West: Part II

"If we aren't vigilant, cyber crime will turn the Internet into the Wild West of the 21st century,"

Janet Reno, U.S. Attorney General (1998)

One hundred years after telegraph wires snaked across the U.S. continent, new technologies converged once again to revolutionize the conduct of business around the world: the microchip, the desktop computer, and the nascent Internet.

In 1969, The U.S. Department of Defense funded a network research project to facilitate information sharing between geographically distant nuclear physics researchers. Two years later, the "ARPANET" project was deemed a success when four universities briefly communicated through networked computer terminals.

As new network tools and applications were developed, tested and refined in the next decade, more universities in the U.S., Canada and Europe connected to the ARPANET, making it the first international network.

Computer scientists and engineers who used the network were delighted. They no longer had to wait days for the postal service to deliver an important research paper from a distant colleague. An electronic copy of the paper could be retrieved through ARPANET in a few minutes time — even if the computer they retrieved it from was thousands of miles away!

If struggling to solve a knotty physics problem, a researcher only had to type out a single query, send it to an appropriate newsgroup such as

Internet Milestones

1970: Electronic Mail (EMAIL). Text messages could be transmitted to recipients across the ARPANET. Researchers appreciated ease-of-use, informality and rapid transmission of messages.

1980: The User's Network (UUNET). Distributed Bulletin Board Systems (BBSs) provided decentralized communication between geographically distant users. Using a modem and telephone, a participant could log into UUNET to leave a message and to read other users' responses. Messages were typically grouped by topic into "newsgroups." By 1999 there were tens of thousands of newsgroups participating.

1983: The Transmission Control Protocol/Internet Protocol (TCP/IP) networking procedure was formally adopted by ARPANET and all supplementary networks connected to it. Collectively those systems become "the Internet."

1988: Internet Relay Chat (IRC). Users anywhere in the world could "converse" in real time with other users through exchanges of typed messages.

1988: Search engines were developed to categorize, index and sort through the massive amounts of knowledge that was accumulating: text files, images, and databases.

1989: Mailing Lists (Listservs). An automated process that enabled an email message to be transmitted to multiple users who had interest in the same topic.

1989: First Public Internet Service Provider (ISP): The World.com offered dial-up Internet connection services available to the general public.

1990: Management turnover. US Department of Defense moved classified data to its own network, MILNET, turning over management of the Internet to the National Science Foundation (NSF) through its network, NSFNET. At its peak, NSFNET connected more than 4,000 institutions and 50,000 networks across the Unites States, Canada, and Europe. Commercialization restriction is lifted.

1991: World Wide Web (WWW). The development of hypertext computer language and launch of "The Web" provided easy access to information.

1992: Multimedia: First audio and video multicasts were successfully demonstrated online.

1993: Web Navigation Software (Browsers). The earliest web browser, Mosaic, and later its commercial version, Netscape, incorporated text, sound and video into an easy-to-use graphical application that neatly integrated three Internet technologies: web, email, and newsgroups.

1995: NSFNET transferred management of the Internet to independent organizations.

"alt.physics" and request feedback from other researchers. Replies from colleagues were often immediate.

By 1983, networks, computers and network software applications switched to a standardized communication protocol called Transmission Control Protocol/Internet Protocol ("TCP/IP"). With that changeover, ARPANET began to be called the "Internet." In 1984, the numbers of terminal hosts ("users") reached 1,000 and still even more universities signed on. By 1989 there were over 100,000 users.

The Internet was no longer the exclusive domain of scientists and engineers using arcane computer languages on mainframe computing systems. Their orderly world was becoming more chaotic: Students, unsupervised and relatively undisciplined, were now flocking to the Internet, logging on from desktop and laptop computers.

In November 1988, a 23-year-old student named Robert Tappan Morris introduced code into the Internet network, as part of a research project he claimed he was conducting. Morris intended for his self-replicating "worm" code to measure the size of the Internet. Unfortunately, the code was flawed and caused thousands of computers logged onto the Internet to become inoperable.[16] The "Morris Worm" story was extensively reported in the news.

Other, more sinister characters began to probe deeply into the Internet. In his novel, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, author Clifford Stoll described a network intrusion incident that occurred in 1986. Stoll recounted his tedious but patient tracking of an intruder through a university network and into various military computers on MILNET. Stoll traced the illegal activity to Markus Hess, a 25-year-old German citizen who was recruited by the Russian KBG to hack into and steal sensitive information from US military computing systems. Stoll experienced a great deal of frustration in attempting to gain the interest and investigative support of law enforcement:

> Stoll contacted various agents at the FBI, CIA, NSA, and Air Force OSI. Since this was almost the first documented case of cracking (Stoll seems to have been the first to keep a daily log book of the cracker's activity) there was some confusion as to jurisdiction and a general reluctance to share information (Stoll quotes an NSA agent as saying, "We listen, we don't talk").[xii]

The fledgling Internet was not built to guard against such attacks and penetrations. Internet engineers were given pause to consider what the long-term impacts might be. Network security became a hot topic of discussion.

World.com, the first commercial Internet Service Provider (ISP) in the United States, began offering dial-up connectivity to the public in 1989. Any World.com customer with a computer

[16] Robert Morris was tried and convicted of violating the 1986 Computer Fraud and Abuse Act. After appeals he was sentenced to three years' probation, 400 hours of community service, and a fine of $10,050. He is now a professor at Massachusetts Institute of Technology.

and a modem could dial-up, log on, and cruise the Information Highway.

Navigating the complex architecture of the Internet network challenged the skills of individuals unfamiliar with complex computer command line syntax. The introduction of the "World Wide Web" and web browser applications, such as "Mosaic" and "Netscape," helped to propel delighted users from email, to newsgroups, to World Wide Web exploration, all from one user-friendly interface.

In 1990, Department of Defense migrated all classified information to a proprietary network and assigned Internet management responsibilities to the National Science Foundation (NSF). At the end of the year, about 300,000 users were accessing the Information Highway.

The Internet community of users was excited about NSF's plans to open and fully promote the Internet to commercial enterprises.

> From the time the National Science Foundation (NSF) assumed responsibility for the U. S. Internet backbone, they anticipated a transition to commercial use. There were a few commercial ventures in the 1980s, like the Clarinet News Service, CARL UnCover for scholarly documents, and the Computists' Communique electronic newsletter, but the NSF acceptable use policy and Internet culture were largely non-commercial. NSF is phasing out their support, and commercialization is taking off — you can even order pizza![xiii]

The Federal Networking Council (FNC), responsible for coordinating networking needs among U.S. Federal agencies, determined that the Internet was "a critical resource for the national research and education communities" and concluded that the Internet "…should be made available to the widest possible customer/user base with the highest possible level of service."[xiv]

As Internet Service Providers (ISPs) opened for business across the country, growth rates escalated. In 1994, there were three million users perusing 10,000 newsgroups and 10,000 websites. A year later there were 6.5 million users and the number of websites had increased to 100,000.

The NSF quietly transferred its network management responsibilities to independent organizations on April 30, 1995. The Internet's doors were thrown wide-open for commercial business. The times, they were a-changing.

One Internet user ("netizen") bemoaned the changes but also expressed hope for the future:

> The Internet …was formed in an atmosphere of craftsmanship and information exchange, which persists today. … Perhaps more important, the Internet culture supports open communication. People answer questions, make suggestions, and freely discuss a myriad of topics for the satisfaction of participation and perhaps some enhancement for their reputation — the payoffs are not explicit. This barter/gift-exchange arrangement makes for a more comfortable society than one in which every information transaction is explicitly compensated, and no

> accounting is needed. This open culture is subject to abuse, but it has persisted for years on the Internet. Will increased commercialization end openness? Must it? Can we find policies that balance openness and marketplace efficiency? Social predictions are difficult at best, and the global nature of the Internet makes them even more difficult.[xv]

At the end of 1996, the Internet community consisted of 12.8 million users and a half million websites. The Internet was primed to become Wild Wild West (version 2.0).

The Wild, Wild West: Part III

The dynamics of global growth are changing at least as profoundly as they did with the advent of railroads or electricity. The evolution of the Internet as a pervasive phenomenon means that the traditional factors of production — capital and skilled labor — are no longer the main determinants of the power of an economy.[xvi]

Business Week Online (1999)

In 1994 Forrester Research predicted Internet sales would grow to $4.8 billion by 1998.[xvii] Only a few years later an even rosier economic forecast was reported:

> People are becoming more comfortable with the technology, and businesses are pushing web transactions as a way of reducing costs and increasing efficiency. Efficiency and competitive pricing in the Internet's "frictionless" marketplace are expected to dramatically increase business-to-business sales over the Internet. Richard Prem of Deloitte & Touche expects business-to-business transactions alone to exceed $300 billion by the year 2002. Forrester Research has predicted total web sales of $1.45 trillion by the year 2003.[xviii]

The business community had finally awakened to the huge market potential in Internet sales and the rush was on. It was "Internet or bust!" Everyone wanted a piece of the action and to flaunt the newest status symbol: a web address.

Amazon.com opened a virtual bookstore in 1994, promising customers an enormous selection of new and used books. In 1995, "eBay" started an online auction service where users could sell items by way of the Internet, and later introduced "PayPal" payment processing for online vendors. PayPal customers could send, receive, and hold funds in 17 currencies.

All manner of goods could be ordered from the Internet and delivered by regular mail or express companies. A few Russian websites even offered mail-order brides! Stock brokerages went online, as did financial institutions. The Associated Press, CNN and other news media began to distribute information across the Internet.

Online chatrooms spawned friendships, romances and sometimes even marriages. On the seamier side of the Internet, pirated software, hacker's tools, and child pornography images were freely distributed. Concerns were raised about the exploitation of children by pedophiles. Several well-publicized arrests and convictions of huge pedophile rings got the public's attention, but failed to deter the pedophiles. In seemingly endless numbers they continued to slither through the Internet's underground.

Internet users developed their own jargon: IM (Instant Message), LOL (Laughing Out Loud), IIRC (If I Recall Correctly). Special interest groups formed social networking communities, interactive gaming and gambling sites, and discussion forums. Students emailed bomb threats to their teachers and mercilessly harassed other students

online. Grifters traded swindling techniques.

Handheld wireless devices such as “Smartphones” and “Personal Data Assistants” allowed users to “go online” without the need for a telephone dial-up connection. Voice Over Internet Protocol (“VOIP”) telephone services enabled clandestine phone conversations to be held over the Internet — and under law enforcement’s radar.

Huge volumes of email, including junk email (“spam”) and invitations to provide personal information to fraudsters were transmitted across the country and around the world. Express companies delivered commodities that had been purchased online. Commerce was on the move and following the money, so were the criminals:

> The United States economy, including the growing e-commerce aspect of it, is increasingly threatened by cyber economic crime. Multiple studies still show that fraud, security, and privacy continue to be the primary detriment to the growth of e-commerce. Most economic crimes have a cyber version today. These cyber crimes offer more opportunities to the criminals, with larger payoffs and fewer risks. Websites can be spoofed and hijacked. Payment systems can be compromised and electronic fund transfers to steal funds or launder money occur at lightning speeds. Serious electronic crimes and victimization of the public have caused consumer confidence to waiver. These issues have also lead to growing privacy concerns and demands. In turn, the reluctance of the American public to embrace e-Commerce fully is preventing this new form of business from reaching its potential. We are quickly eroding the trust in our society that has been built up over the centuries.[xix]

Anxious to mitigate liability and stop loss due to credit card fraud and theft of company intellectual property and customer information (“data leakage”), businesses began to take security more seriously in the twenty-first century. More robust security protocols and access controls were put into practice. Employee background checks became a more common practice. In-service employee training on security and data protection was initiated and acceptable use policies were drafted and put into effect. Corporations lobbied Congress for more protection.[xx]

Some businesses and government agencies initiated customer awareness “Internet fraud” prevention programs, sending information in mailings and posting notices on websites — to little avail. Increasingly Machiavellian “phishing” and “pharming” attacks continued to elicit personal information from unsuspecting customers.

Opportunistic Internet outlaws used the Information Highway as their personal road to riches. They used high-end computers and stealth technology such as proxy servers, encryption, steganography and phony (“spoofed”) email addresses. They probed for weaknesses in networks and hijacked accounts to harvest information they could further exploit for profit.

> “Around one in four criminals use false identities, with identity theft

being both a means of masking the criminal's own identity and therefore evading detection — as well as a vehicle for committing further fraud at a later date."[xxi]

Teenagers who were bored and looking for excitement were recruited by organized crime into "hacker" (network intrusion), "carder" (credit card theft) and "phreaker" (telecommunication services theft) gangs. Teens had a significant advantage over investigators: time — time to learn and hone their skills. Many were enticed by the promise of large sums of money and scoffed at the idea of being apprehended by law enforcement.

In 2001, Assistant U.S. Attorney Sean B. Hoar referred to identity theft as "the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society, because offenders are seldom held accountable."[xxii]

Perpetrators victimized multiple victims in multiple jurisdictions, making investigations especially challenging. Others operated remotely from safe harbors such as Nigeria and Sierra Leone and made no effort to hide. They knew U.S. law enforcement couldn't touch them.

In spite of the ongoing criminal activities and threats to national security, there was no Internet Highway Patrol to maintain law and order. Police were about twenty years behind the technology curve.

The proliferation of desktop computers and boomtown atmosphere of the Internet took police managers by surprise. It didn't help that commanders were averse to using computers. (Parents were experiencing the same problem at home: kids knew more about computers than the adults.)

The larger police agencies could better afford to keep up with technology but for the most part, it was old technology: dumb terminals networked to mainframe computers. It would be well into the first decade of the new century before most police regularly sent and received email and used the Internet as a resource and investigative tool.

The smaller agencies were forced to make do with what they had—and what they had wasn't much. Some of them didn't have computers, let alone email or Internet connections. The smaller agencies felt "high tech" if they used facsimile machines. It was sadly ironic that grade school students had better, faster computers than most police.

A few investigators had an interest in computers and taught themselves the skills they needed to investigate "cybercrime" and they shared their knowledge with other investigators.

In those days, we were working without resources, real knowledge, or awareness and exposure to computer violations. We were not experts. We worked hard to overcome the critical gap between the knowledge of those investigated and the knowledge of the investigators.[xxiii]

Some of those early law enforcement pioneers would later become founding members of computer crime-fighting associations such as High Tech Crime Investigators Association

and International Association of Computer Investigator Specialists.

Software developer companies responded to law enforcement's request for forensic tools to assist investigators to preserve and analyze digital evidence. Some of the early pioneer-developers were Access Data, ASR Data, Mares & Company, New Technologies, Inc., and Norton Utilities/Symantec.

In September 2000, the National Institute of Justice published results of a survey identifying issues and obstacles that interfered with successful investigation of cybercrime. State and local law enforcement agencies reported they lacked adequate training, equipment and staff to meet present and future needs to combat electronic crime. Among the findings, there was a demand for:

- Uniform training and certification courses
- Development of electronic crime units
- Investigative and forensic tools

Additionally, NIJ reported that "acquiring appropriate investigative hardware and software poses one of the biggest problems, as such tools are often beyond the budgets of most law enforcement agencies. Findings indicated a large gap between the expertise and resources of many cybercriminals and the agencies that investigate them."[xxiv]

Five years later another survey sponsored by NIJ demonstrated that law enforcement agencies were still struggling to get up to speed on the Information Highway: [xxv]

- Most agencies had no digital evidence unit or resource
- Most agencies did not find or collect digital evidence in most of their investigations
- Only half of state and local law enforcement had attended digital evidence awareness and handling training
- A majority had no policies concerning digital evidence

Investigators who had computer forensic analysis training complained that most of their commanders didn't grasp the scope of the problem. Said one investigator, "I finally got enough training that I felt somewhat confident about my forensic skills and they rotated me back to patrol. All that training — wasted!"

Other officers claimed that they were appointed the "computer forensic guy" because they knew how to boot up a computer.

Another investigator complained about the procurement process. "I'd ordered a new computer workstation to use in the forensic lab. It took nearly a year for the purchase order to be approved. The day I got approval was the same day new computer models went out on the sales floors. I was stuck: forced to buy out-dated technology!"

Federal criminal statutes were inadequate and needed updating. For example, federal statute, 18 U.S.C. 1028, addressed the fraudulent creation, use or transfer of identification

documents. There was no provision for theft or criminal use of personal information. Enacted on October 30, 1998, the "Identity Theft Act," contained an amendment that criminalized fraud in connection with the unlawful theft and misuse of personal identification.[17]

As late as 2007, some states still were without criminal statutes to address computer intrusion or identity theft.

Many of the cases involved transnational investigations but police had limited means to seize foreign perpetrators' digital evidence. The formal Mutual Legal Assistance Treaty or Agreement (MLAT or MLAA) processes through U.S. Department of Justice Office of Foreign Affairs was far too time consuming. It took so long to process the paperwork that by the time the legal documents were in order, the volatile digital evidence was no longer recoverable.

Local prosecutors refused to extradite out-of-state suspects for "small dollar loss" cases, even when the combined loss from multiple victims in other jurisdictions was substantial — but not substantial enough to interest federal prosecutors. Federal prosecutors weren't interested in small dollar loss cases, either.

Victims grew upset, feeling that their complaints were ignored, which for the most part they were: 25% couldn't even get the police to take a report.[xxvi] Some agencies played "pass the victim" — local police referred victims to a federal agency, that agency referred the victim to another agency and so on, until finally the victim gave up in frustration.

In another example of "victim abuse," the Las Vegas Sun reported that 300 victims requested assistance through a telephone hotline associated with the Nevada Attorney General's Identity Theft Passport program that was set up to "help identity theft victims clear their name." Not one of the callers received any assistance whatsoever. According to the article, state officials said the lack of assistance was due to a lack of funding.[xxvii]

Meanwhile, the media constantly broadcast news stories about millions of identities being stolen, traded, or lost. Internet sales were dipping. Some customers expressed reluctance to make online purchases and expose themselves to identity and credit card theft, but it didn't really matter. Whether they shopped online or not, their personal information was vulnerable to misuse from myriad sources: mail theft, purse snatching, workplace data leakage — the list was endless.

The problems weren't exclusive to U.S. police; law enforcement officers in other countries were under similar pressures. The London Metropolitan Police Force (the largest police agency in England), called for a national unit to address the problem, warning that the "U.K.'s local police forces can 'no longer cope' with e-crime."[xxviii]

It wasn't all gloom and doom; there were some positive developments.

In 1985, The California District Attorney's Technology Theft Association (DATTA) applied for a grant to "… train San Francisco Bay area investigators

[17] Identity Theft and Assumption Deterrence Act ("Identity Theft Act"), 18 U.S.C. § 1028 (a)(7).

and prosecutors in high-technology theft investigation." One program goal was "To establish an organization base that will provide the nucleus for the development of a regional high-technology theft prevention effort."[xxix] The goal was met in 1986 with the formation of the High-Technology Crime Investigator's Association (HTCIA) with over 30 Southern California law enforcement jurisdictions participating.

One of the first digital evidence analysis courses taught in the United States was Computer Investigative Specialist (CIS) training, hosted at the Federal Law Enforcement Training Center in Brunswick, GA in October 1989. Trainees included criminal investigators from the Internal Revenue Service and the Canadian Tax and Revenue Service. That same month, instructors for the CIS course met and founded the International Association of Computer Investigative Specialists (IACIS).[xxx]

In 1995, the U.S. Secret Service started up a private-public partnership known as the Electronic Crimes Task Force in New York City. It was unique in that it comprised not only local, state and federal law enforcement investigators but also private industry and academia. By 2007, there were "ECTFs" in 25 cities across the U.S.[18] (It was ironic that the Secret Service, established in 1865 under the capable guidance of Allan Pinkerton, should be also the first federal agency — one hundred years later — to gather public and private sector cybercrime fighters together under a single collaborative roof.)

Some local police agencies also sought private sector assistance. In 1998, the State of New York initiated "Operation Sabbatical," an investigation of a group suspected of distributing images of child pornography. Low on resources and skills, the police contacted and vetted a computer user group named "Ethical Hackers" who agreed to provide technical expertise.

> Law enforcement officials obtained 21 search warrants in 14 states and 4 countries, while the members of Ethical Hackers played central roles from their home computers. While warrant-bearing police knocked on doors of suspected members of the ring, the members of Ethical Hackers effectively barred access to a discussion area in cyberspace where child pornographers were known to congregate, flooding it with meaningless data to render it unusable. The idea was that if the members could not communicate, they would not be able to warn one another about the raids.[xxxi]

It was also noted that Internet "netizens" were happy to assist law enforcement with cybercrime investigations, more so than with garden-variety street crime. Perhaps this was so because amateur "cybersleuths" felt more comfortable rendering assistance while safely ensconced in front of computer monitors. (Or perhaps police had so insulated themselves from their

[18] Atlanta, Baltimore, Birmingham, Boston, Buffalo, Charlotte, Chicago, Cleveland, Columbia SC, Dallas, Houston, Las Vegas, Louisville, Los Angeles, Miami, Minneapolis, Newark NJ, New York, Oklahoma City/Tulsa, Orlando, Philadelphia, Pittsburgh, San Francisco, Seattle, and Washington D.C.

constituencies they lost sight of the fact that most citizens were willing to help maintain law and order in their communities — both real and virtual.)

In Florida, the Flagler Beach police department conducted, in partnership with a private sector vigilante group, an Internet sexual predator sting. Twenty-one men, including a police officer, were arrested for attempting to have sex with a minor.[xxxii] Chief Roger Free remarked, "Teaming with private entities is the wave of the future."[xxxiii]

It was the wave of the future? Clearly, Chief Free hadn't heard about Allan Pinkerton.

The Wild, Wild West: Part IV

This is the first time in American history that we in the federal government, alone, cannot protect our infrastructure. We can't hire an army or a police force that's large enough to protect all of America's cell phones or pagers or computer networks — not when 95 percent of these infrastructures are owned & operated by the private sector.
Baley, U.S. Secretary of Commerce (2000)

As we enter into the fourth decade of the technology age, law enforcement must prepare to respond to progressively complex cybercrimes, including information warfare.

> Many states are developing highly sophisticated information and cultural warfare capabilities and exploiting the pervasiveness and pliability of digital information to gain commercial or political advantage.[xxxiv]

Cybercriminals, including terrorists, do a much better job of communicating among themselves than do the police. There is a cultural reason for the difference. Police have traditionally kept information closely held. They are unwilling to share information with "outsiders" — including other police jurisdictions. Neither do most police officers spend appreciable amounts of time engaging in online chat, developing an understanding of online users behaviors, or familiarizing themselves with the Internet underground.

Conversely, cybercriminals spend hundreds of hours online, working to perfect their tradecraft. After testing and validating exploits, hacking into telecommunication systems, or selling stolen credit cards, they freely chat with peers about "best practices."

No longer are young hackers boasting about defacing websites. Now they're involved in much more sinister (and profitable) endeavors. As an example, an as yet unidentified group of "hactivists" deployed virtual armies of computers infected with malicious software "bots"[19] to attack Estonia's government, business and banking systems. Alarmed at the damage to national security, ecommerce and consumer confidence, Estonia's President Toomas Hendrik Ilves announced,

> "It is a serious issue if your most important computer systems go down in a country like mine, where 97 percent of bank transactions are done on the Internet," Ilves said. "When you are a highly Interneted [sic] country like we are, then these kinds of attacks can do very serious damage."[xxxv]

These rogue groups are also responsible for using bot-controlled networks to mass-email Internet users with

"Pump and dump" stock offers and other scams

"Phishing" invitations designed to lure consumers to phony websites and

[19] A "bot" is an automated software program that executes certain commands when it receives a specific input (like a ro-"bot"). "Botnets" are compromised networks of computers that criminals control of to distribute spam (to perpetrate more frauds) or malicious computer code to attack other computers.

trick them into entering identification, banking, and other critical information.[20]

Organized crime groups are actively recruiting talented computer programmers to steal millions of dollars and thousands of identities.

> "Web Mobs" have developed into an international clearinghouse of stolen plastic card and identity documents ranging from passports, driver's licenses to student ID cards. … A very successful international framework has been created for criminals to buy and sell data and share their expertise with each other. Criminals no longer have to be specialists in all areas of fraud. They can simply learn how to steal data and then sell it to someone who manufactures cards and actually commits the fraud, or vice versa.[xxxvi]

At the local level, police have identified a correlation between individual methamphetamine users, identity theft, and organized crime. According to a press release issued in April 2007 by Senator Maria Cantwell, "…the Spokane County [WA] Sheriff found a meth connection in each of the area's identity theft crimes. That same year, Pierce County [WA] officials reported that between 80 to 90 percent of the county's identity theft defendants had either a pending or prior meth charge."[xxxvii]

Further, identity theft and credit card fraud are funding terrorism.

Significant links between Islamic terrorist groups and cybercrime were discovered after "Irhabi007" (aka Younes Tsouli) and two accomplices were arrested and later convicted of inciting murder using the Internet.

This image was found on ikbis.com, an Arabic website. The caption reads: "Evolution of Thieves." (Note: Arabic is read from right-to-left. The photo should be viewed right-to-left)

On one computer belonging to the suspect, forensic investigators found 37,000 stolen credit card numbers along with personal information on the identity theft victims (account holder's address, date of birth, credit balances and limits).

The three terrorists made more than $3.5 million in fraudulent charges using credit cards stolen in phishing scams. In addition, they:

> Compiled shopping lists for items that fellow jihadists might need for their battle against the American and allied forces in Iraq, including global positioning satellite (GPS) devices, night-vision goggles, sleeping bags, telephones, survival knives and tents. Records show the men had purchased other operational resources, including hundreds of prepaid cell phones, and more than

[20] Virtually all spam is now sent from hijacked computers.

> 250 airline tickets using 110 different credit cards at 46 airlines and travel agencies.
>
> Al-Daour also allegedly laundered money through online gambling sites -- using accounts set up with stolen credit card numbers and victims' identities -- running up thousand-dollar tabs at sites like AbsolutePoker.com, BetFair.com, BetonBet.com, Canbet.com, Eurobet.com, NoblePoker.com and ParadisePoker.com, among others. All told, al-Daour and other members of the group conducted 350 transactions at 43 different online wagering sites, using more than 130 compromised credit card accounts. It didn't matter if they lost money on their wagering. Winnings were withdrawn and transferred to online bank accounts the men controlled.[xxxviii]

Investigators in the United States and abroad spent hundreds of hours tracking the trio's financial activities across thousands of merchants in more than a dozen countries.

Police aren't the only ones who are scrambling to catch up with technology; the judiciary is struggling, too. At the "Irhabi007" trial,

> The magistrate overseeing the trial, Justice Peter Openshaw, interrupted the proceedings with a statement that observers said stunned prosecutors for the Crown. "The trouble is I don't understand the language. I don't really understand what a Web site is."[xxxix] (Emphasis added.)

One of the case investigators was reported to say, "There is no law enforcement agency in the world that, if this wasn't a terrorism financing case, would follow up on this. They just don't have the resources."

Another credit card fraud exploiting Voice Over Internet Telephone (VOIP) surfaced in 2006. "Vishing" uses automated dialing and transmission of a recorded message that advises victims their credit card has been used illegally. Users are instructed to call a telephone number to provide account verification by entering a 16-digit credit card number on the keypad.[xl] Other more sophisticated exploits will be developed; VOIP technology is relatively new.

Malware will become more widespread in web pages, videos and on opinion-discussion websites called "blogs."[xli]

Other wide open markets ripe for targeting with malicious bots and phishing messages are mobile devices and smart phones. These threats may especially impact first responders who use mobile technology.

Radio Frequency Identification (RFID) is emerging technology used to uniquely identify objects, animals and persons. RFID chips are being embedded in US and UK passports, credit cards and identification. There is one reported instance of an RFID security probe that successfully scanned and read data on a passport that was sealed in an envelope.[xlii] Vulnerabilities are still being assessed, but it is certain that there will be future attempts to exploit RFID technology.

In 2000, William C. Boni predicted that “techno-crimes… will continue to increase in intensity and sophistication on a massive global scale… the attacks may become so prevalent and vicious that there will be an outcry for governments to take action to stop outrageous violations of international and national laws. These demands for government action will come primarily from businesses, especially those involved in e-commerce whose businesses will be suffering major losses.”[xliii]

The emerging field of digital evidence forensic analysis already threatens to overload police resources, with no sign of easing up. There will be a steady demand for qualified experts who can identify, investigate, collect and analyze digital evidence, both in the public and private sectors. Demand is likely to exceed supply, especially if law enforcement is unwilling to hire non-commissioned personnel.

Pay differential between public and private sectors will negatively impact police recruit applicant pools. Police will struggle to retain experienced investigators and digital evidence examiners because private sector employers will attempt to lure them away with offers of higher wages, better benefits and more attractive workplace environments.

Mass production coupled with dropping prices will enable more consumers to purchase digital devices, increasing the numbers of potential perpetrators and victims.

Devices will continue to shrink in size, but data storage capacities will expand. Easier to conceal, miniaturized devices may not be recognized as evidence repositories or they may be recognized, but overlooked.

Digital evidence acquisition, processing and analysis times will exponentially increase.

Greater amounts of evidentiary data will place demands on police evidence storage facilities. Long-term storage of digital evidence on unreliable or defective storage media may expose agencies to liability if data is lost or corrupted.

Digital forensic training and equipment costs will challenge even the largest law enforcement agencies. Examiners must keep current with forensic software tools and techniques. Further, as new digital devices are marketed and used or abused by criminals, additional new forensic training, hardware, software and human capital will be required to process and analyze the evidence. Procurement cycles must be shortened in order to keep pace with technology.

Because each digital device has its own proprietary operating system, forensic software developers will be unable to stay abreast of production and proliferation of new devices.

As the emerging field of digital evidence forensics matures, there will be mandates necessitating certification and recertification of examiners, adding more costs to be factored into police budgets.

A digital forensic examiner recently commented, “It’ll get worse before it gets better. This is the Wild, Wild West version two-point-oh. We’re on a

runaway train and the outlaws mean to derail us.”

The Wild, Wild West: Part V

Cybercrime, with its global reach, presents daunting challenges to law enforcement, but challenges faced by 19th century law enforcement are essentially no different than challenges confronting 21st century crime-fighters. We can overcome the obstacles and reduce the impact of Internet crime by bearing in mind that there is nothing new under the sun.

By the time I'd finished my research I had only one thought. "We're doomed!"

Fortunately Granddad's adage, that "there's nothing new under the sun," reminded me to look to the past for solutions to future problems.

Twenty-first century investigators can emulate the tactics that Pinkerton and law enforcement investigators successfully used to fight nineteenth century "high tech" crime.

Our agency operates with a less than optimal budget, is under equipped and often understaffed. We may need to look at out-of-the-box solutions to acquire the technology skills, hardware and software we need to stay abreast of cybercrime. Pinkerton's innovative business practices might be worth considering. Some ideas for consideration are:

1. Use innovative hiring practices; screen candidates for performance suitability.

Build a reserve or volunteer cadre of knowledgeable experts from the community who will work under the supervision of experienced investigators to assist in seizure and acquisition of digital evidence. Their strength would be their technical skills; their weakness would be a lack of knowledge of evidence preservation. It may be more cost effective to teach evidence preservation to non-police than to teach digital evidence seizure and analysis to police. Possible sources for technicians are:

- Information and network system administrators
- Computer science teachers or students
- Computer programmers

Qualified candidates could also assist with digital evidence analysis. Some candidates (or their employers) might even pay for their own forensic software training and or certification.

2. Ensure investigators have up-to-date training, equipment and materials.

Procurement Cycles: Meet with civic administrators to discuss ways policies might be revised so that police can keep up with technology.

Needs Statement: Prepare and personalize arguments about how failure to keep up with technology can come back to haunt police and community administrators.[21]

[21] *Sheriff's Office Comments on Kylie Taylor Case* (Clark County Sheriff: Press Release, September 22, 2004) <http://www.clark.wa.gov/news/news-release.asp?pkNewsSeq=420>; (Perverted Justice.com Archives, September 18, 2004) < http://www.perverted-justice.com/?missing=46>; (Corrupted Justice.com) <http://www.corrupted-

Sponsorships: To augment strapped budgets, community or business donations could be solicited. A nonprofit consortium of technology-based businesses could be formed to provide assistance, guidance and support. "Brand marketing" (discrete paid advertising on police equipment, for example) could be a source of funds.

Public Relations: Police can apprise constituents about lack of and need for skills training, hardware and software and request the community's financial support. An open solicitation fund-raising drive may be more successful than traditional tax-based requests. Explain how community will benefit in the long term. Consider using a theme such as "We can't help you if you can't help us fight cybercrime."

3. Make continuous learning a high priority.

Mentoring: Request all personnel to learn about technology trends, new products, threats, and forensic techniques and share knowledge with others.

Newsletter: Create an in-house newsletter that summarizes news articles, surveys, war stories, product reviews, etc. Use email distribution to save printing costs. Judiciary and prosecutors could contribute articles, as well.

Roll Call Training: Technology experts and product representatives could be brought in to give brief talks about their area of expertise (e.g., Internet Service Providers, cell phone company representatives, or bank fraud investigators).

4. Information management should be in a constant state of updating and renewal.

Chiefs Meeting: Discuss regional approach to information sharing. Draw up MOUs once agreements are reached.

Local: Evaluate extent of communication with other jurisdictions. Are we sharing information about possible cross-jurisdiction cases (elderly abuse scams, mail box thefts, etc.)? How can we improve?

Statewide: Are we receiving timely, relevant information from the data fusion center? What needs to be changed to make better use of the data?

Community: What about setting up a text messaging alert system to go out over cellular phones? Amber alerts and BOLOs could be broadcast, with appropriate cautionary warnings. Participants could sign up via the department website.

5. Vision Statement: "We never sleep" (in relentless pursuit of criminals).

---

justice.com/forums/viewtopic.php?t=1437&postdays=0&postorder=asc&start=45>; (North American Missing Persons Network: Kylie Taylor) <http://www.nampn.org/cases/taylor_kylie.html>; (Genderberg.com) <http://www.genderberg.com/phpNuke/modules.php?name=News&file=article&sid=98> Also see Grigoriadis, Vanessa (2007) *'To Catch a Predator': The New American Witch Hunt for Dangerous Pedophiles* (Rollingstone.com Issue 1032 July 30, 2007) <http://www.rollingstone.com/news/story/15723886/to_catch_a_predator_is_nbcs_primetime_dragnet_the_new_american_witch_hunt> Accessed July 31, 2007

Decide upon a vision statement with respect to cybercrime, and then live the vision department-wide. Encourage businesses and citizens to live the same vision.

6. Relationship building.

Cultivate relationships with technology savvy constituents, both in the community and on the Internet. Investigators should learn to use the same tools that the Internet underground uses.

Use community "eyes and ears" (and keyboards) to stay abreast of threats, techniques and crimes in progress. Mentor "netizen" activist groups.

Give community presentations on computer security, fraud, Internet safety, and best practices. (Use experts if officers do not have the knowledge so that they, too, will learn.)

7. Know thy enemy.

Develop online informants. Learn about technology uses and abuses from the people who use the technology. A good place to start is with students; they're likely to have the latest technology products and to be learning about exploitations and abuses. User groups might be another resource.

8. Prevention.

Police to Business: Can we build a network with businesses via email or Internet web page? This could be an avenue to distribute crime bulletins and "in progress" alerts and request for assistance notifications. Notices about Internet crimes such as phishing, credit card thefts, etc., that impact our community could be broadcast.

Police to Citizens: A similar website could be built to jump off the police-to-business website. Information about Internet scams, and fraud prevention tips as well as neighborhood crime watch notifications could be distributed either via the website or email.

Insist that citizens and students become the first line of defense. Show them how. Lead by example.

9. Public Relations.

Be honest with the community. Share successes, but also failures.

Send a message to the criminals that cybercrime will be treated no differently from street crime and aggressively prosecuted.

.

---

[i] Keating, Anne B. and Hargitai, Joseph R. *A Guide to Incorporating the World Wide Web in College Instruction.* (New York University Press 1999) p 13

[ii] (n.d.) *Wiring the Continent: The Transcontinental Telegraph Line.* IEEE The Virtual Museum. <http://www.ieee-virtual-museum.org/collection/event.php?id=345680 7&lid=1> Accessed May 2, 2007

[iii] Ross, N.E. (1928) *How to Write Telegrams Properly.* <http://www.telegraph-office.com//pages/telegram.html#How%20to %20Save> Accessed May 2, 2007

[iv] Wynn, William R. (n.d.) *The Telegraph Romance and Bushwhacking Mystery* (Unusual Family Stories (of White & Cleburne Co.)) <http://www.rootsweb.com/~arwhite/unusual .html> Accessed March 5, 2007

[v] Clay, Wallace (1969) A. *The Life Of A Telegraph Operator On The "Old C. P." In The Golden Spike Era.* (Oral History 1969). <http://www.nps.gov/archive/gosp/research/ pappy_clay10.html> Accessed March 12, 2007

[vi] Norfolk Southern Police Department. *History of Railway Police.* <http://nspolice.com/history2.htm> Accessed March 15, 2007

[vii] Pinkerton, William (1893) *Highwaymen of the Railroad.* The North American Review (November 1893) Legends of America: A Travel Site for the Nostalgic & Historic Minded. <http://www.legendsofamerica.com/WE-RailroadHighwaymen.html> Accessed March 31, 2007

[viii] Pinkerton, William (1893) *Highwaymen of the Railroad.* Ibid.

[ix] Waite, Donald E. (1977) *The Langley Story Illustrated: An Early History of the Municipality of Langley.* (D.W. Friesen & Sons Limited, Altona, Manitoba: November 1977) p 173

[x] Geringer, Joseph (n.d.) *Allan Pinkerton and His Detective Agency: We Never Sleep: The Wild West.* Court TV Crime Library: Criminal Minds and Methods. <http://www.crimelibrary.com/gangsters_outlaws/cops_others/pinkerton/5.html> Accessed April 9, 2007

[xi] Geringer, Joseph (n.d.) *Allan Pinkerton and His Detective Agency: We Never Sleep: The Wild West.* Ibid.

[xii] *The Cuckoo's Egg (book)* (n.d.) Wikipedia, the free encyclopedia <http://en.wikipedia.org/wiki/The_Cuckoo's_Egg_(book)> Accessed July 8, 2007

[xiii] *Commercialization of the Internet* (1994) (Communications of the ACM, Vol 37, No 11, November, 1994) <http://som.csudh.edu/fac/lpress/comm.htm> Accessed July 7, 2007

[xiv] *FNCAC Resolutions* <http://www.nitrd.gov/archive/fnc-material.html> Accessed June 22, 2007

[xv] *Commercialization of the Internet (1994)* Ibid.

[xvi] *The Internet Economy: the World's Next Growth Engine.* (Business Week Online. October 4, 1999) <http://www.businessweek.com/1999/99_40/b3649004.htm. Accessed July 9, 2007

[xvii] *Commercialization of the Internet* (1994) Ibid.

[xviii] *The Growth of Internet Sales, Continued* (n.d.) <http://www.taxpayfedil.org/igrowth.htm. Accessed July 7, 2007

[xix] Gordon, Dr. Gary R. and Curtis, Dr. George E. (2000) *The Growing Global Threat of Economic and Cyber Crime* (National Fraud Center. December 2000) pp 9-10. Available at <http://www.lexisnexis.com/risksolutions/conference/docs/cyber.pdf> Accessed May 3, 2007

[xx] Sarkar, Dibya (2007) *Big Names Team up to Lobby against Cyber Fraud* (MSNBC.com July 26, 2007). <http://www.msnbc.msn.com/id/19980384/> Accessed July 31, 2007

[xxi] (2007) *Cybercrime Goes Back 50 Years, Says BCS Expert.* (Public Technology Net: E-Government and Public Sector IT News) <http://www.publictechnology.net/modules.php?op=modlead&name=News&file=article&sid=7960> Accessed February 28, 2007

[xxii] Hoar, Sean B. (2001) *Identity Theft: The Crime of the New Millennium.* (U.S. Department of Justice: United States Attorneys' USA Bulletin. March 2001 Vol. 49, No. 2) p 3

[xxiii] Levin, Yanir (n.d.) *Analyzer in Israel – Investigator vs. Hacker* (MYPI Services.) <http://www.mypi.co.il/articles/analyzer-in-israel-investigator-vs-hacker/> Accessed July 9, 2007

[xxiv] Stambaugh, H; Beaupre, D, Icove, D., Baker, R Cassaday, Wayne and Williams, W.P. (2000) *State and Local Law Enforcement Needs to Combat Electronic Crime (National Institute of Justice: Research in Brief*. U.S. Department of Justice: Research in Brief, NCJ 183451 August 2000.) p 2

[xxv] Appel, Edward J., Pollitt, Mark W., (2005) *Report on the Digital Evidence Needs Survey Of State, Local and Tribal Law Enforcement* (Joint Counsel on Information Age Crime, Inc. and Northeastern University College of Criminal Justice for National Institute of Justice. March 2005) p 3

[xxvi] (2006) *President's Identity Theft Task Force Interim Recommendations* (September 19, 2006) p 6 Available at <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf> Accessed May 23, 2007

[xxvii] Pratt, Timothy (2008) *ID theft victims feel burned by state's 'hotline'* (Las Vegas Sun/Sun News, June 28, 2007) <http://www.lasvegassun.com/sunbin/stories/text/2007/jun/28/566622574.html> Accessed June 29, 2007

[xxviii] Espiner, Tom (2007) *U.K. Police: We're Overwhelmed by E-crime."* (CNet News: January 26, 2007) <http://news.com.com/2100-7348_3-6153743.html> Accessed January 26, 2007

[xxix] Smith, John C. (2001) *History of HTCIA.* (History of the High Tech Crime Investigation Association) <http://www.jcsmithinv.com/HTCIAhistory.htm> Accessed July 14, 2007

[xxx] King, Pamela (2007) *History of IACIS*. (IACIS Newsletter, Issue No. 1. 2007) p 2

[xxxi] Richtel, Matt (2000) *In the Pursuit of Cybercriminals, Real Detectives Rely on Amateurs* (New York Times: May 17, 2000) <http://query.nytimes.com/gst/fullpage.html?res=9802E1D81F3BF934A25756C0A9669C8B63> Accessed July 10, 2007

[xxxii] (2006) *21 Arrested in Central Florida Predator Sting* (Local6.com News: December 12, 2006) <http://www.local6.com/news/10519503/detail.html> Accessed July 15, 2007

[xxxiii] Garrett, Ronnie (2007) Internet Watchdogs (Officer.com: Law Enforcement Technology, March 2007) <http://www.officer.com/publication/article.jsp?pubId=1&id=35694> Accessed May 22, 2007

[xxxiv] (2007) *The DCDC Strategic Trends Programme 2007–2036* (UK Ministry of Defence, Development, Concepts and Doctrine Centre (DCDC), January 2007) Available at <http://www.mod.uk/NR/rdonlyres/5CB29DC4-9B4A-4DFD-B363-3282BE255CE7/0/strat_trends_23jan07.pdf > p 61 Accessed April 2, 2007

[xxxv] McKinnon, John D. (2007) *Estonia Presses Bush for Cyber-Attack Research Center* (The Wall Street Journal Online: Washington Wire June 25, 2007) <http://blogs.wsj.com/washwire/2007/06/25/estonia-presses-bush-for-cyber-attack-research-center/> Accessed June 27, 2007

[xxxvi] (2006) *Organized Crime Driving Card Fraud to New Heights of Profitability* (CUNA Mutual Group: Press Release, June 22, 2006) <http://www.cunamutual.com/cmg/newsReleaseDetail/0,1252,15837,00.html> Accessed July 15, 2007. And Leland, John (2006) *Meth Users, Attuned to Detail, Add Another Habit: ID Theft* (New York Times, July 11, 2006) <http://www.nytimes.com/2006/07/11/us/11meth.html?ex=1153540800&en=7b6c7773afa880be&ei=5070>

[xxxvii] (2007) *Committee Clears Cantwell Measure to Investigate Link Between ID Theft and Meth: Cantwell Study Included in Comprehensive Anti-Identity Theft Package* (Press Release of Senator Cantwell, April 26, 2007) <http://cantwell.senate.gov/news/record.cfm?id=273186> Accessed July 15, 2007

[xxxviii] Krebs, Brian (2007) *Terrorism's Hook Into Your Inbox: U.K. Case Shows Link Between Online Fraud and Jihadist Networks* (WashingtonPost.com) <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153_pf.html> Accessed July 5, 2007

[xxxix] Krebs, Brian (2007) *Terrorism's Hook Into Your Inbox: U.K. Case Shows Link Between Online Fraud and Jihadist Network* Ibid.

[xl] Jaques, Robert (2007) *Cyber-criminals switch to VoIP 'vishing'* (Vunet.com, July 10, 2006)

[xli] Thomas, Vinoo (2006) *Hackers Use Wikipedia as Bait* (McAffe Avert Labs Blog November 7, 2006)<http://www.avertlabs.com/research/blog?p=128> Accessed Mar 22, 2007

[xlii] Kirk, Jeremy (2007) Crack! Security expert hacks RFID in UK passport (Computer World: Security March 6, 2007) <http://www.computerworld.com/action/articl

e.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&articleId=9012406&taxonomyId=82&intsrc=kc_top> Accessed March 8, 2007

[xliii] William C. Boni and Kovacich, Gerald L. (2000) *Netspionage: The Global Threat to Information* (Butterworth-Heinemann: Massachusetts) p 238

In the lawless "Old West," outlaws robbed banks & held up trains:

Toby M. Finnie & Earl Moulton

1800s	TRANSPOR-TATION	ORGANIZATION	TECHNOLOGY	COMMUNICA-TION	COMMUNITY	INVESTIGATION	FORENSICS	LAW	PREVENTION
U.S. Law Enforcement	• Rode horses & used horse-drawn conveyances	• US Army had jurisdiction over territories • US Marshals were few & far between • Formed specialized groups such as railroad police • Deputized private investigators • Deputized citizen posses	• Had limited access to new technology • Printed & distributed illustrated wanted posters	• Shared information via telegraph (1851) & telephone (1877)	• Were sole enforcers, sometimes with little, inconsistent, or no community support • Citizens formed vigilance groups (some turned vigilante, meting out frontier justice)	• Collected evidence, interviewed witnesses & victims • Analyzed telegram headers for leads	• Fingerprint identification	• Pacific Railway Act • Used extradition processes to bring outlaws to justice • Enacted state & federal legislation	• Incarceration • Public hangings
Canadian Law Enforcement (RCMP)	• Rode horses and used early US railways	• Established in 1873 as formal policing agency modeled on Royal Ulster Constabulary acting as sole LEA in advance of settlement	• Complete lack of technology, reliance on US telegraph services – reliance on Metis and Indian translators	• Reliance on US facilities until 1885 then reliance on public telegraph • Used by Gov't to scout telegraph routes	• Formal authority preceded settlement and had full community and First Nations support	• Acted as investigative, judicial and custodial authority	• Reliance on eyewitness *viva voce* evidence	• Imported British law and authority	• Used existing Metis and First Nations leaders and lots of discretion to introduce new legal system
U.S. Private Sector	• Transported large sums of money & commodities via railroad, overland & coaches & express wagons	• Employed armed guards as agents & express men • Hired private sector investigators who were not constrained by jurisdiction	• Used telegraph & railroads to increase business revenue • Purchased & supplied high powered hand guns & rifles to enforcement & security personnel	• Used telegraph to coordinate arrival & departure of trains & shipments • Used "wireless" telegraph overseas • Advertised & marketed via telegraph	• Investigators gathered & analyzed information about outlaws from community	• More manpower, flexibility to act quickly • Used women as investigators • Investigators used crime analysis, geo-mapping, & criminal profiling • Used undercover operatives; covert operations	• Fingerprint identification	• Lobbied for federal jurisdiction over train robberies • Pursued outlaws across borders & into foreign countries • Extradition laws revised	• Designed stronger safes • Used physical access controls to protect shipments • Investigators educated business owners; provided mug shots & criminal profiles • Warned of certain capture & prosecution of suspects
Canadian Private Sector	• Banking system moved west with after legal authorities well established	• Jurisdiction extended over 1/3 of continent only constrained by US border	• Made do without	• Utilized only in rarest of circumstances	• Officials only engaged in investigations	• Not Used	• Not used	• RR PD est. 1885 – confined to RR property only	• Not used
U.S. Outlaws	• Rode horses & used horse-drawn conveyances	• Formed outlaw gangs such as the James Brothers, Dalton Brothers, & the "Wild Bunch" • Recruited family & friends. • Used aliases & disguises	• Hired expert safe crackers • Used explosives & smokeless powder	• Cut telegraph wires • Conspired via telegraph • Carefully planned robberies	• Often received encouragement, support & shelter from community • Recruited & mentored young men • Threatened witnesses • Wounded or killed innocents	• Gangs split up to elude investigators • Hid out in remote areas	• Wore gloves & masks to evade detection	• Escaped across state lines or borders to evade capture • Bargained release by promises to "go straight"	Fear of loss of freedom or life
Canadian Outlaws	• Used expanding US rail network to access goods and alcohol for trade into Canada	• Outlaws occasionally rode into Canada but returned on encountering formal authority and lack of community support	• Limited or no use	• No organized groups requiring communication	• No community support as coummunity was comprised of settlers & ranchers	• Not an issue	• Very little face to face crime requiring disguise	• Had certainty of outcome with formal system	• Certainty of process and outcome

In the Lawless "Old West" of the Internet, online outlaws rob banks and customers:

1900s	TRANSPOR-TATION	ORGANIZATION	TECHNOLOGY	COMMUNICA-TION	COMMUNITY	INVESTIGATION	FORENSICS	LAW	PREVENTION
U.S. Law Enforcement	• Few agencies proactively patrol the "Information Highway	• Form special investigative groups such as USSS Electronic Crimes Task Forces (US) & Serious Fraud Office (UK)	• Some agencies use Internet as investigative tool • Some agencies cite equipment, personnel training costs as insurmountable barrier • Make no attempt to be proactive	• Most communicate via telephone, email & cellular phones • Some use PDAs, text messaging • A few use encrypted email, & secure web portals or VPNs	• Too few officers spread too thinly to adequately patrol the Information Highway • Citizens begin to form vigilance & vigilante groups	• Investigators overwhelmed by sheer numbers of fraud cases • Take complaints, rarely follow up with investigation • May suggest victims contact federal LE • Federal LE take complaints but rarely follow up • Huge demands on LE resources • Offender data not collected	• Computer & network forensics exams conducted by a few agencies • A few forensic software applications are in use • Digital video forensics is introduced	• DAs refuse to bring action due to jurisdictional issues • Multiple small-dollar loss victims reside in multiple jurisdictions • MLATS process too slow • National ID Theft Task Force established	• Ad hoc development of programs by interested officers
Canadian Law Enforcement (RCMP)	• Lack of resources , knowledge, skills and priorization of persons crime reduces focus on Cybercrime	• Specialized units slowly developed	• Skills, abilities developed to be successful but with little capacity to handle volume • Proactive overwhelmed by reactive needs	• Communica-tion and information access controlled by IT personnel without full regard to operational needs	• Community lack of knowledge keeps demands for service relatively low	• Only very limited capacity to pursue cases • Evidence gathering impeded by existing evidence and jurisdictional law	• Forensics capabilities lag behind the need •Lag time is increasing	• Limited availability of knowledgeable prosecutors and judges • Legislative process unable to keep pace with technology	• Ad hoc development of programs by interested officers
Private Sector	• Transport large sums of money via computer networks & the Internet •Financial institutions close accounts that are breached by fraud • Institute broad strategies for handling data leakage	• Hire in-house investigators (often former LE) • Employ IT security professionals & consultants	• Lax operational security practices with respect to online banking operations	• Telephone & cellular phones, plain text &/or encrypted email, PDAs, text messaging, web boards, VPNs, portals • Some use VOIP	• Costs of fraud passed onto merchants • Consumers charged higher interest rates • Targets of burglary are wallets & credit cards; not electronic goods	• Intrusion cases investigated • Fraud loss is cost of doing business • Traditionally thought to be uncooperative with police	• Employ investigators with CFE training • Rely on network administrators to conduct investigation	• Lobby against tougher regulatory statutes • Privacy rights advocates protest data analysis & monitoring	• Some attempt to educate consumers about best practices
U.S. Cybercrime Outlaws	• Use the Internet Highway as a road to riches • Continue to "follow the money" (via new tech such as smart phones, Voice over Internet Protocol, GPS) • Bot-infected computers controlled by "bot herders" act on behest of organized criminals to attack on broad scale	• Organized crime, terrorists involved • Form distributed networking groups to share exploits, exchange credit card & ID theft information • Pay for development of spyware & keyloggers • Opportunistic use of social networking sites such as MySpace.com	• Exploit emerging technology to assist in criminal activities • Devote hundreds of hours to perfect skills; take advantage of mentors	• Telephone & cellular phones, VOIP with encryption, email (with encryption), steganography, PDAs, text messaging, web boards, blogs, IRC • Use technology to contact & coordinate group activities	• Receive encouragement , support & validation from online peers • Recruit & mentor others to participate • Share best practices information, data, exploits • Develop new tools to perpetrate crimes • Develop new ploys to defraud consumers	• Act with impunity • Use encryption, steganography, proxy servers, obfuscated email addresses & operate from safe haven countries to elude detection & arrest	• Use anti-forensics (encryption, data shredders & obfuscators) • Hide information via steganography	• Aware that jurisdictional problems work in their favor • Fear of prosecution not a deterrence • Privacy protection laws favor criminal • Light sentencing not a deterrent	
Canadian Cybercrime Outlaws	• "MafiaBoy" a "script kiddie" hacker, has far-reaching impact	• Process and procurement capabilities far outstrip those of LEA	• Criminals are the epitome of early adopters	• Quick identification of emerging communication technologies	• Creating own communities of interest • Limited external impact means further extremist positions	• Exploit jurisdictional and time constrants	• Use IT to distribute both knowledge and tools to thwart LEA	• Exploitation of existing laws	

In 2000, things began to change…

2000s	TRANSPOR-TATION	ORGANIZATION	TECHNOLOGY	COMMUNICA-TION	COMMUNITY	INVESTIGATION	FORENSICS	LAW	PREVENTION
Law Enforcement	• "On scene" investigations often consist of remote acquisition of evidence • Digitally "patrols" the Information highway via spiders & bots, noting deviancies & abuse patterns in communication traffic • Becomes proactive as well as reactive; concentrating on prevention rather than just prosecution	• All LE officer-recruits are trained to recognize digital evidence devices; applicable criminal statutes; & can protect digital crime scenes • Organize citizen Internet Patrols "CIPs" to act as eyes & ears, reporting suspicious activity to Data Fusion Centers (DFCs) • Police proactively use social media and the eyes & ears of consumers to "patrol" the Internet & identify antisocial behaviors, fraud trends, perpetrators & victims	• Data Fusion Centers (DFCs) promote real time decision making by multiple jurisdictions • Procurement processes changed • Increased demand for reliable data retention & storage capabilities • Powerful catalogue, index, search & retrieval software developed • Digital fingerprints are required authentication	• Victim's complaints are self-reported onto a Universal Police Report that is verified by any PD prior to submitting it into it's system • Decentraliza-tion: Cases are assigned to investigator(s) according to codified indicators, which may involve multiple investigators working in different geographic areas • Information shared via secure wireless telecommunicat ion systems	• Citizen vigilante groups are organized, & trained to work directly with law enforcement • Law enforcement relies on citizen groups & business owners to identify trends, target perpetrators & prevent escalation of fraudulent activities. • Voluntarism accepted in the analog world will become acceptable in the digital world	• Computer forensics now includes remote acquisition & analysis of data • With court authorization, critical cases are forensically analyzed in real time • Solid state devices enable terabytes of data to be stored as evidence • Statutory changes address both volume and timely nature of digit evidence	• Through data fusion centers, forensics capabilities & assistance flow down to even the smallest police agency • Digital evidence retention & reliable storage capacities & lengthening times for forensic analyses present unique challenges • Standards for both tools and practitioners will emerge	• Council of Europe's Convention on Cybercrime Protocols ratified by 100 nations • Countries agree to enable swifter collection of digital evidence, render mutual assistance, & share information • Best form of "law" will set out the basis for continual change of the law	• Citizens receive government sponsored best practices training upon purchase of digital devices • State/Federal governments enact "shall issue" user licenses that put onus for safe operation & use of digital devices upon citizen-users; compel manufacturers & software developers to make low cost training programs available to purchasers • Call-home mechanisms enable LE to track & recover stolen digital devices. • Changes made to the underlying protocols – SMTP etc. – to better enable processes of authentication, non-repudiation and data integrity
Private Sector	• Routinely store & transport financial & other sensitive data on networked computers • Businesses must certify that employees use best security practices through training & testing	• Citizens participate in CIPs & report suspicious activities • Financial Institutions work directly with LE	• Newly developed AI-driven technologies track usage patterns & deviancies • Mechanisms embedded into systems & software enable tracking • Will continue to drive the development and rollout and applications of new technology	• Businesses may routinely track & anonymously report abuse patterns, virus attacks, etc to DFCs	• Citizens attend digital device workshops, earn certifications in security • Schools compel students to use best practices to secure user license	• Businesses regularly work with LE to prevent & prosecute digital criminals • Prevention is prioritized over prosecution	• Enables product encoding & RFID tracking to prevent piracy & copyright violation • Retains data files, images & surveillance videos		• Threat of banishment from digital devices becomes effective deterrent • Development of new detection & analysis technologies
Cybercrime Outlaws	• Rely less on Internet & more on mobile technology such as smart phones, PDAs • Commission of offences for the purposes of technology , e.g."happy slapping," etc)	• Use Internet to share information, communicate & plan • Exploit vulnerabilities	• Continue to stay a few paces ahead of LE • Increased social stigma against cybercriminals	• Facilitate mass mobilization ("flashmobs") via real-time sharing of information	• Form temporary alliances • Contract-hire rogue programmers • Use encrypted devices	• Adopt more sophisticated encryption & activity-cloaking techniques to counteract detection	•Employ anti-forensics • Use full disk encryption to impede forensic examination	• Surveillance of society challenges privacy, civil liberties	• Threat of loss of access to digital devices deters criminal activity