White Paper

The Arrival of the Network Armies

The Effect on Public Policy And Marketing

Industry and government in the United States are addressing the task of dealing with ICT (Information and Communications Technologies) and its primary attribute, the Internet. The power of the Internet as a communications and marketing tool has become recognized as mission critical and is causing upheavals and reengineering throughout most industrial sectors and government agencies.

This document presents a look at the decentralized phenomena known as Network Armies and proposes that a focus from the perspective of various user groups, along with the use of methodologies such as Cybernetics, will yield new and unimagined benefits in marketing and communications, new potential for private ownership of data, and a new paradigm of individual control in communications and marketing.

Implementation of the ideas posited will result in substantive public policy considerations and will create a new sector on the Internet (C2B), with related political and monetary issues.

Keywords
Network Armies, Hub Activity, Hub Entities, Cybernetics, ICT, new economics, consumer profile, Metcalf's Law, Reed's Law.

Author
Thomas Brannon

Correspondence: tombrannon@hotmail.com

White Paper

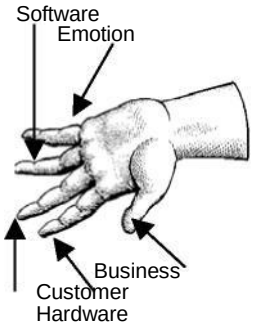
Contents

Appendix

PRESENT STATE

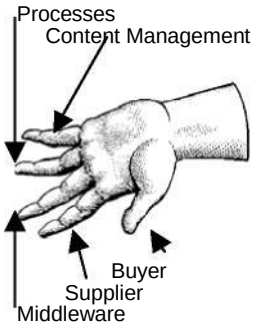
The Five Fingers

The Internet is a sufficiently young technology that methodologies, best practices and taxonomies are still evolving or emerging. Those who create the content are generally trained in a "prior" discipline such as graphic arts, computer programming, or instructional design. An Internet composite skill-set has been emerging, however, and new directions are most apt to originate where the emerging Internet skill-set resides. This new generation of Internet creators are those who possess skills in five areas of one hand or the other (B2C or B2B) of the Internet strawman:



B2C

- *THE BUSINESS — In-depth knowledge of the business of the enterprise owning a Website or of the related industry sector.*
- *THE CUSTOMER — Knowledge of the customers of the business or sector.*
- *HARDWARE — An understanding of the technical aspects, TCP/IP, networks, code languages, HTML, XML, firewalls, data transmissions, etc. Everything the customer doesn't see.*
- *SOFTWARE — The design and content aspects, everything the customer sees. This includes software, creative arts, information research and design.*
- *EMOTION — Often not acknowledged. Here is where the customers feels, then acts. The user experience equals user knowledge. And if the first four are successfully handled, user error will never occur.*



B2B

- *THE BUYER — The enterprise owning the purchasing process.*
- *THE SUPPLIER*
- *MIDDLEWARE — The technical side of B2B, most often providing cross platform connectivity for client/server access and scalability.*
- *PROCESSES + TRANSACTION ELEMENTS — The design portion of B2B.*
- *CONTENT MGT + CUSTOMER SERVICE — The final element, replaces the EMOTION element of B2C.*

It is rare that a Website is designed with equal attention and skill in all five areas. In fact, most eCommerce sites are noticeably deficient in several primary elements. Add to this a consumer hesitancy due to privacy concerns and the lack of an electronic customer service philosophy and you have the current state of many Websites following the collapse of the dot com sector in April, 2000.

Why did the collapse occur? Among other events, during the initial excitement, eCommerce was pushed to the forefront like a rose blossom, picked and held close to our face so we could see its beauty and smell the fragrance. But a picked blossom lives only momentarily and when it faded, we panicked, failing to see the flowers growing all around us. The Internet is, and will continue to be, an important part of the landscape. And its importance is growing as ICT (*Information & Communication Technologies*) works out ways to improve everything from customer-assisted processing to communicating product information and promoting ease-of-purchase.

Technology Assumptions

There are several assumptions key to the ideas and conclusions in this White Paper. These are emerging as maxims, generally accepted as true in most all cases and functioning as guiding principles.

1. TECHNOLOGY DRIVES BUSINESS

   There is effectively no area of industry that is not infused with, run by its technology and systems (desktop and legacy). If it can be automated, computerized or robot-enabled, it's a safe bet to assume a competitor is doing it (or is about to).

2. LEADING TODAY'S TECH CYCLE IS THE SENSOR

   During the last three decade-long tech cycles, we've seen the primary focus on (i) microprocessors, (ii) laser/fiber optics, CD-ROM, (iii) sensors. The current cycle of sensing technologies is mission critical, predictive, risk controlling. Sensors produce data that is essentially free and current use includes such activities as assembly-line robots, camera surveillance/biometrics, and CRM marketing (collecting customer profile data for data warehouse marketing).

3. CHANGE IS ACCELERATING

The new rule is that the past is irrelevant. Companies are encouraged to become cannibals; Intel goes from memory chips to microprocessors. Increases in the rate of acceleration used to be perceived as chaos! Where survival might be vital to a manager, it's immaterial to investors. This is hard to argue against when a subsidiary is worth more than the parent! A recent remarkable non-fiction book, *Creative Destruction*, revealed that, in the 1920s, the average age of an American company was 65 years — in 1998 this had shrunk to ten years.

4. THE INTERNET DEMONSTRATES GENERAL SYSTEM THEORY

All systems share certain characteristics allowing them to function as a system. The Internet "system" has a distributed command and control design. Where command and control is distributed, the system is a network of sub-systems, each with its own local environment and independently stable. The sub-system can withstand much higher levels of stress than a single-hub, centralized system. Its user community thus has much more autonomy and control in using it. The only requirement for success in multiple self-stabilizing sub-systems is some level of coordination and communication — to enable use of required standards, for example.

5. CUSTOMER DATA IS A VALUABLE ASSET

One of the most ubiquitous aspects of eCommerce is the collection of all possible customer and user data. This information is stored, segmented, organized, analyzed, and often sold as an ancillary product in the vast majority of Internet transmissions. The public has come to understand this and has evolved a schizophrenic attitude, hating the practice, rebelling against it on one hand and willingly participating in return for the slightest benefit on the other.

It is clear that companies value consumer profile data so highly they're going to court, suing even the government, to retain rights to use the data as fully as possible.

Business Benefits

To the extent that consumers have embraced the Internet, it cannot fail. This "embrace" produced $60 billion in online sales in 2001. And for this reason, some ecommerce initiatives will continue to be business critical for American companies - which cannot afford to abandon these initiatives, knowing that competitors are ready to fill the gap. And all of this is the source of consumer empowerment. In fact, this may even become recognized as a maxim of business. It might go like this:

> *The consuming public for products and services has decided, approved and participates in the use of the Internet for communicating and for transacting activity for all products and services*

If this is true, a number of assumptions can be stated and proven, including:

1. *Geographical boundaries in industrial relations and consumer marketing are increasingly more transparent.*
    - *This justifies a global approach*
    - *Local governments are increasingly losing power*
    - *The proper approach may be regional (by continent) or cut by language.*
2. *The Internet is a strong impetus for related economic and business ideas, such as making a case for global or regional currencies.*
3. *The growth and strength of network armies" will continue and accelerate.*
4. *As these armies" (which are simply groups of people, sharing common purpose-driven goals) grow and cause perturbations, they will become recognized, authenticated and legitimized (Network Armies discussion follows).*
5. *Entities will arise to provide various services to these ad hoc network armies.*
6. *Technology is a feature of many of the characteristics of all the above stated assumptions. To the extent this is true, Cybernetics is the appropriate tool to address the attendant issues and opportunities*

Companies using technology and the Web have experienced such benefits as*:

- Reducing distribution costs (sometimes to nearly zero - re: low-cost airlines)
- Reduced ad costs (P&G used the Web for new product introduction of a tooth whitener, reached their first year sales target in six weeks)
- Reduced costs in building brand (a BMW Motors project reported savings of $25 million in costs compared to reaching the same result without the Web)
- A large grocery retailer achieved savings of 1% of total sales using shopper data to target promotional offers

NETWORK ARMIES

Before addressing the subject of Network Armies on the Internet, the network effect itself must be understood. A network is a system of individual points (nodes) working together or joined in some way, sharing a commonality such as function, makeup, or the layer in which it's classified. Robert Metcalfe, developer of Ethernet and founder of 3COM, first wrote about the valuation of the network of telecommunications customers. He pointed out that the value is the square of the number of customers and that this number grows exponentially while the cost per node stays the same or diminishes. That is, two people on a party-line can make two calls (to each other) while an increase of six additional users creates 64 possible calls (eight people all able to call each other).

Industry has either not grasped the import of Metcalfe's Law, or has discounted it , for good reason. The economic value derived by the seller is not where the true value lies. The phone company, after all, is only selling six more telephones in the above example, not 62 more.

Then, David Reed (Internet engineer and MIT software guru) stepped up to explain the benefit in a different way — ascribing the value to the consumer side. The 64 telephone network users in this example won't spend every waking hour calling everyone possible on their telephones, but have the ability and the right to do so. This right is much like a stock option — the ability to perform the action in the future — without any obligation.

(DAVID REED) "Group forming is, in my opinion, the technical feature that most distinguishes the Internet's capabilities from all other communications media before it. Networked communities that support group-forming are growing in scale and reach, and network architectures that enhance group-forming processes are still being invented. Anyone who is serious about the Internet must learn to 'get' the power of group-forming communities."

The typical time when an Internet user steps up to exercise this option is when there is a purpose-driven reason to do so . . . working toward some goal. For Reed's discussion of the corrected meaning of Metcalfe's Law, see http://www.reed.com/gfn/.

Reed's Law is vital to understanding the concept of Network Armies. This new enabling of community, of groups of people with common concerns, is leading to group empowerment and causing concern (if not excitement) in government and industry.

Network Armies Defined

The term seems to have been used first by Richard Hunter, VP Security Research for GartnerG2 and author of *World Without Secrets*. The purpose-driven reach toward common goals presents a powerful metaphor for Internet activity and examples are increasingly easy to find. Perhaps most interesting is the disparate nature of those working on some common goal. In fact, Network Armies utilizing the Internet as a major tactic have only the goal in common and may even be unaware of each other's existence as they exercise their growing power.

(R. HUNTER) "Our era is seeing the rise of the 'network army,' a social structure tied together by values and beliefs, not geography. The network army communicates via the Internet. Its members are drawn from multiple communities. Their agendas may differ dramatically ... but (when in alignment) the army's power can be massive."

Hunter provides examples of this power. One obvious example is al-Qaeda. Another (the virtual opposite of al-Qaeda) was the network of librarians who forced Harper-Collins to change their decision to delay publishing *Stupid White Men and Other Reasons for America's Decline* in the aftermath of September 11th. Then Richard Hunter makes an astonishing statement . . . "negotiation isn't an option because there is no leader in a network army."

The Internet may not even be the primary tactic. A fascinating example occurred in Nashville, Tennessee in early 2002. A budget shortfall led to maneuvering on the State's first income tax. Legislative leaders aligned their lobbyists, their power base and considered it all but finished. A groundswell of protest built up, centered around conservative local radio talk show hosts. Protesters rallied daily by driving their vehicles in circles around the legislative building, honking horns and letting politicians see (and hear) them. The Internet played its part in coordinating events and enabling communication. It was a "network army" event, nothing more than honking their horns and awareness of this network of voters protesting an income tax. Legislators shuttered their offices, called out the State Highway Patrol and gave up. The single issue, and decentralized protest, turned the income tax certainty to defeat.

Communities

The social and behavioral sciences have long been involved in the study of the interactions of people tied together in groups, neighborhoods, communities and networks. The Internet's ability to promote online communities has led to a trend to consider all these communities as networks. Internet communities tend to be far-flung, global and, perhaps, harder to identify as sharing commonalities.

Analysis of social networks has historically looked first at relationships. With network armies, the relationships are ancillary; the primary target is examination of common purpose-driven goals. Interestingly, some of the goals of the largest networks today exhibit the attributes not of groups, but of private individuals. Issues such as privacy, identity theft, personal medical rights, consumer profile data, safety and security — these all comprise very large network armies. And a primary agent in the formation and activity of these networks is the Internet. On the Web, tens of millions of Americans share their experiences in community chat rooms, email newsletters, bulletin boards, and specific eCommerce chat areas. Large, online/TV shopping channels such as Home Shopping Network and QVC adjust their schedules, product features, prices and presentation scripts based on dynamic feedback from shoppers. Many on-air product spokespersons follow their show with time in the chatroom, sharing stories, answering questions and collecting valuable CRM data.

Attention to the dynamics of people networks on the Internet is rare in most Western nations today. A 1996 management White Paper on Organizational Network Mapping described internal staff network mapping at most companies as "subterranean" and "unmanaged." There's even less attention to external mapping of customers. Although this may seem incredible, it's true; Sears announced in July 2002 the development of its first integrated database of customer data for such mapping. And the CRM software industry is barely in the toddler stage, with notable exceptions such as the large customer databases at Wal-mart and General Motors/GMAC.

Remembering that the Network Army is functioning via a command and control structure that is decentralized, and that there is no visible leader in front of the parade, then there are only two elements required to coalesce the army to effective action. There must be a process for communication inside and outbound, and an element of coordination must be available. These are both sought and accepted by viable Network Armies. The communication/coordination activity may be initiated by members/volunteers or provided by some outside source, although entities specializing in outside assistance are not presently apparent — with the possible exception of related offerings from advocacy groups.

It may be that Network Armies arise in an organic fashion, appearing as a matter of course once the elements necessary for existence have been gathered. The primary component, always present at the initiation of every Network Army, is the issue or goal of the network. This is *a priori* and no Network Army can exist without the goal. It is also generally true that the goal is a substantial one, and, since the network is so disparate, the goal will generally be substantive from an economic, political, societal or similar large-scale perspective.

Given these characteristics, it seems irrefutable that, once Network Armies are recognized as a present phenomenon, their attributes and power will be intensely interesting to industry and government. And unless the goals are frivolous, Network Armies will occupy center stage where they exist and can be expected to very often be successful in realizing their goals.

Where the goals of a Network Army are not aligned with industry or government (or the other relevant parties to the issue), there will be a natural conflict and a risk that the other party is unable to fashion solutions meeting the network army's goal. An example of this is in the area of privacy related to consumer profile data. It will always be in a company's best interest to collect as much data as possible and to use this data in the widest possible way. This will always be in conflict with the Army's goals.

Internet consumer privacy makes an easy and clear example for the inherent conflicts in network army negotiations. A primary tool for Network Armies in reaching their goal has generally been to turn to the government to regulate a solution. As Network Armies become identified and additional tools of coordination and communication are provided, less reliance on government will result. In some cases, the mere existence of such a group has been sufficient to reach the goal. New tactics will likely require support services to somehow be fashioned to provide the coordination and communication needed by the network. This can be expected to lead to the formation of new businesses or added services by Internet service companies. How such companies can derive revenue from such services will be a challenge.

It could be argued that marketing strategies addressing network armies will reach closer to the ultimate eCommerce goal of a customized response to a mass market than any other current strategy. Such strategies aimed at network armies will provide early initiators with exclusive access to the various armies.

Given the attributes in the discussion above, Network Armies can also be expected to lead to a resurgence of interest in Cybernetics. This is discussed in the following section.

CYBERNETICS

The science of cybernetics deals chiefly with communication and control as these occur in the interaction between man and machine. The science is fairly young and is of particular significance for those investigating the Internet, its effects and importance to community, politics and economics.

Somewhat related to General Systems Theory, cybernetics is most easily defined while keeping General Systems Theory in mind. Among the rules that govern most systems and sciences are those rules common to all: communication, coordination, feedback loops and adjustments. These rules, taken together, form their own system (i.e., General Systems Theory). The specific science designed to study these common rules is cybernetics.

Most science deals with matter and/or energy while cybernetics deals with form and pattern. It owes much to the military, tracing its roots to a WWII study of the error and correction feedback loop created by advanced anti-aircraft guns, faster airplanes, pilots and gunners. Norbert Wiener, through his book on cybernetics (1948) is credited with establishing the science.

New businesses and directions that evolve following the arrival of the network armies may find that the purest and most successful business models will be based upon a simple Cybernetics approach. Where Network Armies come to be identified via the Internet, the application of cybernetics will yield fascinating results via the provision of coordination and communication required for network activities.

Focusing on how systems function, cybernetics examines the control and communication activities in complex, self-organized adaptive systems such as the Internet. It also shares certain characteristics with the Web. Circularity is important to each, with no preference for hierarchy — using causation, feedback, iteration and self-reference. Processes are explained in terms of the organization of the network manifesting the process. Regulation is based on feedback loops and the effort of equilibrium or striving toward a goal. Finally, instead of force or singular necessity, there is multiplicity of information, alternatives, differences, choices, and networks.

PRIVACY

The effects of the army on private ownership of personal data

In 1991, Ronald Coase was awarded the Nobel prize for economics. His field was a combination of common sense business rules, and the power of the inevitable where things happen because they should. An early methodology involved asking businessmen why they did something a certain way. The output of his thinking, the Coase Theorem, was a kind of social efficiency based on the logical activities of Market Theory. His work provides a valuable lens through which to view how data is owned and used on the Internet. Companies have assumed that data derived from transactions with a customer belongs to the company. Coase's position on personal data and the Internet could be expected to go something like this: "Once the property rights to this data are defined and settled, an efficient solution will follow — no matter which side owns this data." Put another way, the law of property will determine the owner of a thing. The effects of the marketplace will determine how it is used.

Vanderbilt Law Professor Steven Hetcher, in his article "*The Emergence of Website Privacy Norms*," argues similarly for a "compatibility thesis" where "consent" and "use" learn to live peacefully together. To this, Professor Hetcher adds the element of duty and respect for a person's autonomy *.

It is in the area of property rights to personal data that the network army might be expected to raise its powerful head in the future. To date, case law has not treated the consumer very well. Truthfully, the consumer has significant obstacles to overcome in asserting privacy rights toward personal data revealed via the Internet. Fourth Amendment rights are constrained and do not typically pertain to what a person knowingly exposes to the public. Here, in the handful of Internet privacy cases, courts have held that citizens are voluntarily giving up data when they sign up for ISP service, enroll in EFT programs to pay bills online, etc. This is contrary, say the courts, to any assertion of ownership rights, action to protect such rights, or deriving any benefit from such data — hence no legal protections for personal data that finds its way to the Web. The other avenue of risk to privacy lies in the user assuming the risk, knowing full well that their data is leaking out all over the place, again without being able to present any proof of acting against such "leaks."

* See Stephen A. Hetcher, *The Emergence of Website Privacy Norms*, in Michigan Telecommunications and Technology Law Review, Vol 7, 2000-2001

The consumer, in actuality, may be said to be a victim of the technology. There's no method for Web entry other than an ISP. Users must use the search engines and other common tools to navigate. And clickstream data is deadly, with the content mixed into the metadata in a granular revelation against which the user is helpless.

The FTC has attempted to educate the public in America on the subject. It also published the gold standard — the Five Principles of Privacy*. To date, not a single business is known to have adopted this standard, which is consumer-friendly and would be much more expensive than the current opt-out policies. More important, it would transfer substantial control of the data to the customer. And government cannot be expected to legislate this standard; this is not a government obligation, absent substantial and obvious injury to the public at large.

* The FTC Five Principles of Privacy are:

1. Notice/Awareness
2. Choice/Consent
3. Access/Participation
4. Integrity/Security
5. Enforcement/Redress

This is a sensitive, high-profile subject for a large majority of Internet users. The World Wide Web is all about data and Internet privacy is not about recognizing the entitlement; it's about recognizing the value of the data. The market learned first and embraced the opt-out concept. What this means to the current state of consumer data on the Internet is that consumers interested in consent, empowerment, control and awareness need to determine how they can assert their rights and then do so vigorously because (i) the data is out there and will continue to be there, (ii) the data has substantial marketing value, and (iii) consumers will not be able to effectively seek redress when damaged unless they have taken action to obtain legal rights to the data. Something new will have to happen to provide assistance to consumers. The C2B sector will always direct its strategies in ways contrary to these rights.

The federal law establishing opt-out privacy protection for the general public (aka Gramm-Leech-Bliley) is considered a failure at protecting consumers from anything and, in fact, generally has the opposite effect. A brief analysis is included in the Appendix, below.

If the privacy network army determines a method for sharing in the value of its members' data, the tide will turn, the courts may be convinced to recognize data ownership on the part of the person generating the data, and the army can celebrate a victory.

OTHER NETWORK ARMIES

The Investor Army

Mid-2002 is an especially propitious time for considering the existence of the Investor Army. If fact, the discussion may be vital in framing a new approach to the effects of lower stock values and management integrity issues in the market. What are the goals of the Investor Army? If Richard Hunter of Gartner were asked the question, he might come up with these: (1) to be dealt with honestly, (2) to feel that the management of "their" company was working on their behalf (or at least on behalf of the company itself), (3) to be successful in their ownership/partnership with the company as evidenced by positive company income, dividends and stock prices.

HUB ACTIVITY —

Communications and coordination to a specific network, occurring at the network hub and digested by the network

Because of the speed and dynamic updates to investor information available on the Internet, hub activity is occurring that is producing a transformation in the concept of companies being publicly held !

Before this "upgrade" to hub activity, communications and coordination of the investor network was generally: (1) controlled by management, (2) on a cycle that was annual [shareholders meetings], (3) through agents also controlled largely by management [stockbrokers, analysts, reporters, TV shows, etc.], (4) absent investigative [board room] reporting.

The shift in control and timeline is virtually a 180 degree change. The Investor Army is moving toward their purpose-driven goals the only way they can, by canceling their owner participation. Ownership characteristics of publicly owned companies have profoundly changed — possibly forever [i.e., as long as the network exists]. Until the Investor Army is recognized and its goals addressed, recovery is at risk. While it is true that the recovery risk contains operational factors arising from technology (and these are also vital to recovery), the primary elements are human and are more dependent upon the Investor Army goals than on anything else, including the Fed, interest rates, GDP, housing starts, unemployment figures, war with Iraq, security, etc.

Recovery may be possible without attending to the Investor Army, but, if the Investor Army model is authentic, there will be no substantial recovery until hub activities begin to turn around the negative position on Investor Army goals. An examination of recovery strategies seems to confirm the Investor Army/hub idea. Management certification of financial reporting, for example, is in alignment with probable goals of an Investor Army.

NC3 Marketing, the company initiating this White Paper, identified the Investor Army in second quarter 2001. A number of events confirmed the network; one of these was the computer hacking of proxy voting forms at a Vivendi annual shareholders meeting. In addition, public concern (growing to outrage) was building over the unconscionable compensation packages at many companies.

The hub activity that has occurred cannot be undone. Given the three probable goals of the network, stated above, there will have to be new and extraordinary solutions sought, and vigorous regulatory activity is probable.

The goals dealing with honesty and ethics will provide the greatest challenge for CEOs and senior management. Stock option programs have been especially prone to abuse. One CEO at a high-tech company [the leader in its sector] managed to bump his annual salary of $300,000 up to $35 million annually for the past six years using options. And the way these were reported in financials made last year's actual 29% drop in earnings look like a 21% increase. Adding insult to injury, the CEO converted every single option to cash; he owns zero stock in his company. The Investor Army will demand that CEOs everywhere work toward higher share prices for the right reason rather than to simply reach the strike price so they can cash in their options.

Anecdotal evidence such as this is being communicated at this moment throughout the Investor Army. Those concerned with recovery include every member of the network, and these members will fight to achieve their goals. They've already begun — the levels in the market are the result.

Additional Latent Armies

Identity Theft — An emerging network that is closely related to the privacy network is made up of citizens concerned about identity theft. In early 2002, the Federal Trade Commission announced such theft comprised over 40% of all complaints to the agency and had become the fastest growing crime in America. Gartner Group followed with a study showing that as little as 25% of identity thefts had been reported to the FTC and the scope of the problem was likely much larger than FTC estimates.

Substantial research, time and expense is required for individuals to monitor and cure any theft events from their records (8 to 18 months and over $700 by some estimates). Hub activities delivered to network members could greatly shorten the time and reduce costs. The sense of community in dealing with being a victim would also enhance psychological recovery. While it is true that the majority of identity theft activity is neither high-tech nor concerned with the Internet, recovery activity lends itself to automation and Web communication techniques.

Additional groups worthy of consideration for common purpose-driven goals and identification as network armies include (data from Census 2000):

Disabled	54 million Americans with $175 billion of discretionary income
Single person, no children households	168 million Americans (60% of population)
Post-retirement Americans	50 million plus, projected to increase to 79 million by 2015
Hispanics	Over 35 million, projected to double by 2030
Vehicle Owners/Operators	100 million plus

PUBLIC POLICY IMPLICATIONS

Hub entities will find themselves up against public policy issues rather quickly. Research from a cybernetics perspective on technology, its effects and trends as these pertain to society, industry, government and the citizenry will be the first task for the hubs. From this will follow establishment of relationships with the armies. Services and products to assist networks in reaching goals will then evolve. In some cases, revenue may result which could be passed through or shared with the network.

The hub will also assume some leadership activities on behalf of the armies. One chief area here may involve setting up alliances with universities, consumer interest groups and researchers. This would be vital to addressing the complicated social issues that will arise. An example is the U.S. Privacy Army task on data ownership — legal issues, Constitutional considerations, case law, etc. New technologies will be used, such as emerging database models; the Associative data model as a replacement for relational databases is an example. This will require alliances with academic IT research groups and departments.

If the network army model is valid and if Richard Hunter's description is correct (latency, size, power, no visible leader), then a myriad of issues and challenges flow naturally. These will require a broad base of assistance and will impact many areas of public policy, national and international.

MARKETING

Network Army

Recognizing the consumer army may have a major impact on marketing, including the primary marketing mission of achieving a customized response to a mass market. Wal-mart provides a powerful example of the potentials for cybernetic network army marketing. The giant retailer seems to be considering its customer base as a goal-directed consumer army. First, it has been pointed out many times that Wal-mart is unique in representing its customers more than its suppliers. That is, if we ask a Wal-mart supplier whether they consider Wal-mart part of their sales force or as a customer, most suppliers state that dealing with the retailer is more like selling to a frequent (and demanding) customer.

Assuming standard consumer goals such as best quality at the lowest prices, Wal-mart has been able to exhibit the same goals in its mission. It is therefore fulfilling "hub" duties on behalf of its customer base and is favoring the network over any individual customer or supplier.

The retailer is also dynamically monitoring the customer base for early identification of customer trends and segments, their size and attributes. In doing this, they constantly sample the network. In fact, Wal-mart is noted for its database development and large customer data warehouse. It's also noted for events such as the highest single day sales of any retailer in history - $1.25 billion USD on the day after Thanksgiving, 2001.

The recognition and organization of network armies would open entirely new avenues for marketing of products and services. By identifying the purpose-driven goals of a network, the marketing relationship presented could be highly integrated with network goals. Network army hubs (organized central coordination and communication entities) would also pass marketing content to the network that was 100% permission-based. It could be argued, in fact, that most of today's marketing strategies would be enabled for a reach that was both higher-level and deeper. New models of permission-based marketing would result. Imagine the network/hub version of email 100% permission marketing where, rather than agreeing to receive an email transmission, the network agrees to review the contents, then click through and review links and to receive the service/product material offered. Visionaries such as Seth Grodin, author of *Permission Marketing*, may have begun to sense the network armies and deal with them.

Imagine the following steps added to the development of every marketing program:

1. Consider the user group as a network army
2. Identify and examine probable purpose-driven goals
3. Reconcile the network army profile to the projected user group profile

This will strengthen the customer profile, remove those who are included for any reason other than sharing the network goals. In the purest sense, demographic data on customers becomes immaterial except for internal reasons related to production, delivery, etc.

The end result will probably enlarge the customer base, enable global marketing and strengthen customer ties to the product.

If the network army model is valid, then it's both transformational and a tool for marketers who wish to remain where they are. If the model can be shown to be congruent with such retail successes as Wal-Mart, then business ignores the network army at its own peril. There's more money in staying where we are, they may say, because that's where everybody is . . . or are they?

Network army marketing tactics share elements with economic behavior (EB) concepts. Those working with EB may be early supporters of network army marketing and may be expected to enhance research in this area.

If network armies are invited to participate during the formation stage of new products and new companies, the effect could be stunning. Imagine AARP members invited to assist with the creation of a new HMO for senior citizens. Imagine the network army being there when Ford and Qualcomm formed their Wingcast joint venture, intended to implement rich telematics services in Ford products. Imagine the network members telling Wingcast, "We don't care about in-car email reminders when a band whose CDs we purchased at Amazon.com is playing in our city and voice reminders that we're only two blocks from a billboard advertising the concert. We do care that our car tells us when the tire pressure is low." Would Wingcast have folded (June 2002) if the network had been able to communicate its goals in this area?

To the extent that network armies break down geographical borders, we might see entirely new models of economic activity. Imagine an Internet currency, eMoney, so that network members could easily conduct online trade everywhere. A third-party entity such as Verisign could administer the system, help set currency values and establish electronic accounts into which network members could transfer funds. An individual's eAccount (similar to the debit card model) could function as a commodities account where goods could be purchased online. This could be very attractive in countries such as Russia, where citizens find it difficult to locate goods and it's not uncommon for citizens to bury money rather than deposit it in an uncertain banking environment.

In the Americas, imagine that retail stores establish online purchasing CPUs at cashier stations, conduct a retinal scan and instantly transfer eMoney to the customer's store account. The customer is able to experience the product and get instant possession. The store is a fulfillment center for the online purchase, has fewer employees, perhaps fully automated online cashier stations and reduced need for knowledgeable staff. There could also be a central, in-store SME (subject matter expert) center where a customer can go online to a webcam assistant.

Any network member could shop in a common environment, anywhere in the world. All businesses would compete equally and inexpensively. What's new here is the global view of commerce that comes into view by recognizing and accepting the network army concept. Such discussion also introduces the need to consider anything ancillary to the functionality of the network army, such as currency.

A critical requirement to recognizing and enabling network armies is the establishment of hub entities, those business groups, Websites, etc. that will coalesce a network and provide coordination and communications in furtherance of the network goal. At least one such entity is in the formative stages. NC3, a startup located in Tennessee, has announced plans to conduct specialized market consulting in the area of network armies. NC3 plans include the use of cybernetics and new database design in assisting the several network armies it has identified.

CONCLUSIONS

What is required to move ahead with research and action regarding network armies? The primary enabler seems to be the hub that will fulfill coordination and communication duties for the networks. The hub model shares some characteristics with advocacy and public interest groups. Perhaps the purest example is *Consumer Reports*. An important effect of hub activity will be the birth of an entirely new sector on the Internet, C2B. Websites launched by hub entities will likely use the portal model of Web development and will resemble AARP's relationship to senior citizens.

The ability to identify and aggregate large groups on the Internet carries its own value. An interesting example of this valuation is the story of Mirabilis, an Israeli company started by several young men in the early 1990s. They were Internet geeks who locked themselves in a warehouse with a promise to come up with something that was needed by people using the Internet. They invented instant messaging and began to give it away as shareware. Today, it's still free, shareware software; but, when they reached critical mass of over 12 million avid fans in 1996, AOL paid them between $300 and $400 million for their company — telling them to simply continue giving away the program.

Hub activities have the potential to take marketing to the next-higher level — because hubs will be positioned in a close partnership with network army members. A partnership similar to, but even more substantial than, Wal-mart's relationship with its customers. This partnership will empower network members and pass along to them benefits that are currently leaking away, or being paid to the wrong recipients (ad agencies?) or that are so far unrecognized.

APPENDIX

Gramm-Leech-Bliley (Federal Opt-out Law)

To anyone interested in Internet privacy and the protection of consumer data, the Gramm-Leech-Bliley Act (12 CFR Title V ["GLB"]) has been held out to offer the protection of federal requirements for companies to develop a Privacy Policy, a method for individuals to demand their data be kept secret and various steps for providing a notice of these rights. The law went into effect November 13, 2000 but compliance was voluntary until July 1st. In the summer of 2001, all of America received notice documents from the various companies they do business with.

But GLB is about much more than Internet Privacy. Described by industry groups as enabling the greatest growth for financial services in over a half century, GLB was written by the banking industry to expand its financial services marketplace. The Act itself states the purpose is to "enhance competition in the financial services industry by *providing for the affiliation of* banks, securities firms, insurance companies and other financial service providers, and for other purposes." It permits the formation of holding companies to engage in *all activities determined by the Federal Reserve to be `financial in nature" or incidental or complimentary to a financial activity*. [Emphasis added]

Speaking before the Financial Services Subcommittee of Congress, Richard Parsons (Exec VP, Bank of America) represented the Financial Services Roundtable. His testimony demonstrated the excitement of the business sector over GLB. The Roundtable, he said, "strongly supports" the regulation because it's good for business, good for the consumer, and it demonstrates that various businesses (such as real estate agencies and car dealerships) should be defined as financial activities covered by the Act.

A Forrester survey on privacy (Why Privacy Matter$) found that, while only 44% of privacy-concerned Internet users are aware of GLB, only 17% of those who were familiar with it are confident that its provisions afford them protection regarding their personal data, and 80% felt the Opt-out notices were unintelligible.

APPENDIX

Federal Regulation

Financial Services Modernization Act of 2000

GLB is actually detrimental to consumer privacy interests on the Internet. A case can be made for this based on a number of points, including:

- The Opt-out platform is facing the wrong direction! The default condition in the Act is that all the nonpublic personal information gathered on someone **can** be shared with nonaffiliated companies (including being sold to them) *unless* the consumer reads the company's procedures for making his demand to hold the data private — and takes the required actions to do so.

- The Opt-out process is often confusing. The required steps may be detailed and failure to follow these exactly negates the request. One Fortune Five company has a "Privacy" link to their corporate Statement but a second link at the end of the long legal Statement must be found and followed to the Internet Policy page where a third link (at the end) takes the reader to the Opt-out forms and directions. Pages must be printed, filled out and faxed or mailed to a particular location.

- Sharing data with "affiliated" firms requires no Opt-out, In other words, data **may** be shared in spite of any desire of the consumer. The meaning of "affiliated" is very broad and apparently can be interpreted to include any other company whatsoever that has any contractual connection with the company. This statement is based on an assumption that a firm will generally only relate to other companies in the normal course of their business and any third company that assists in marketing, servicing, processing, protecting, or responding to a customer's account or purchase is a case where the customer has no Opt-out rights.

- The nature of the information is defined to benefit the companies' position. Data that could be developed from any public investigation is not covered by GLB. Such data as a customer address and phone number that may be located in a Telephone Directory is not protected data.

- Companies may revise their data sharing practices, publish a revised Policy Statement requiring a new response and thereby expire any previous Opt-out request.

- There are other exceptions when not even the notice itself is required. [1]This type of exception is at § 313.15 of the Act:

	§ 313.15 - The requirements for initial notice do not apply when you disclose nonpublic personal information: (1) With the consent or at the direction of the consumer; (2) (i) to protect the confidentiality or security of your records pertaining to the consumer, service, product, or transaction; (ii) To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (iii) For required institutional risk control or for resolving consumer disputes or inquiries; (3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with industry standards, and your attorneys, accountants, and auditors; (4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq) including State insurance investigators. (5) To or from a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or (6) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit.

Finally, companies seem anxious to be a part of GLB, to publish their Privacy Policy and Opt-out forms, saying "Look at us, we're acting to protect your privacy on our Web site." Companies don't volunteer to be regulated unless they benefit from this.

<End>