The Significance of the Frontier: Why Privacy and Cybersecurity Clash
James Andrew Lewis

The internet diminishes privacy. Perhaps it will ultimately destroy it. The effect of digital technology on an individual's ability to control personal data raises serious concerns, but does disappearing privacy also mean the end of civil liberties? Not necessarily, and understanding how to preserve political liberties while privacy shrinks is an essential task for the digital future.

But privacy has come to mean more than the protection of personal data. Jerry Berman, one of the grand old men of privacy describes the Internet as a "revolutionary force."[1] Privacy today is not just preserving individual control of personal data, Privacy means preserving the original sense of unlimited opportunity the internet seemed to offer, as an unconstrained space for individual action.

The expansive definition focuses privacy policy on three issues. The first is grounded in the traditional understanding of privacy and seeks to limit the effect of network technologies on individual control over personal data, retaining as much as possible of our pre-internet seclusion. The second is to reduce or constrain the role of government in cyberspace, to protect civil liberties. The third is to safeguard the internet's potential for innovation. Privacy policy asserts that these three are linked and depend on defending an open and free internet.

Many assumptions underpin these assertions. The most problematic are that we can restrict or eliminate government involvement in the internet without risk; that anonymity is always beneficial; that an open, unsecure internet is crucial for innovation, and that digital technologies have not eroded earlier conceptions of privacy as it has done with so many other concepts in business and politics. In looking at these assumptions, we must ask if trends by in technology and governance have made some aspects of privacy policy obsolete.

The privacy debate takes place in the context of the powerful political effect of digital technologies, which is reshaping concepts of allegiance and legitimacy – the acceptance by citizens of a government's right to exercise authority over them. These changes in turn reshape views of the relationship of the state to privacy and civil liberties. Privacy provides the terms for a larger political debate over the role of government, government's loss of legitimacy, and the increase in public disillusionment and distrust that has marked politics since the 1960s. These trends shaped pioneering notions of internet governance and the internet community's relation to the state. Differing views of authority, economics and the role of government explain why cybersecurity initiatives so often meet with opposition from the privacy community and why cybersecurity can be seen as detrimental to civil liberties, innovation and economic growth. The central issue in the relationship between privacy and cybersecurity is trust in government.

A history of cybersecurity policy would show the close relationship between the idea of the internet that must remain untrammeled - a self-organizing community where states have only a limited role - and the largely feckless cybersecurity measures adopted by the U.S. over the last fifteen years. Preserving an unconstrained internet has been the primary objective for U.S.

[1] Colin J. Bennett, The Privacy Advocates: Resisting the Spread of Surveillance, MIT Press, 2008, P. 50

policy for the three administrations that have grappled ineffectively with cybersecurity.[2] These ideas leave the United State more vulnerable than potential opponents who do not carry this ideological burden. More importantly, they limit our ability to define problems and to identify new solutions.

Other nations once accepted unquestioningly the pioneering American vision for the internet, that it was borderless, works better without government intrusions, and is innately open free. These concepts are now being rejected and replaced. New approaches to cybersecurity will require governments to extend sovereign control into cyberspace. This expanded role will lead to extending law, regulation, and sovereign control into cyberspace; developing international agreements on responsible behavior; and the adoption of active defense measures by individual nations or even groups of nations.

Even without the incentive of security, many nations are eager to assert sovereign control. Cyberspace will become like any other global infrastructure, with rules and institutions for governance where governments play a major and leading role. The risk in this extension of sovereignty is that there are increasing challenges to the values of openness, free access to information, and free speech. The larger problem, however, is that the American perspective on privacy and internet governance is unique, and as the governance of the internet, once largely dominated by American, shifts to a global community of nations, the result of continuing to advocate old ideas is that the U.S. will lose the influence it needs to defend core values for the rules, institutions and technologies of the internet.

The new approaches to cybersecurity clash with the vision of cyberspace that is reflected in the work of many privacy organizations. Changing attitudes toward legitimacy make the connection between the privacy community and cybersecurity complex and largely antagonistic. It helps to understand this by considering the legacy of the battle over control of encryption software. The fierce battle over encryption policy shaped the relationship between the privacy community and the government and helped cast it in decidedly antagonistic terms.

I. The Crypto Wars Shaped Privacy and Cybersecurity

At the opening of the Internet age, the U.S., alone among industrialized nations, controlled encryption products as a munition for export purposes (and export controls provided some influence over the domestic market). When encryption had been a hardware product sold mainly to the banking industry and to friendly governments, these tight controls were not a problem. The advent of personal computing and the internet allowed messages to be encrypted by software, rather than specialized hardware. The Internet and e-commerce offered a giant new market for encryption software. Munitions controls restricted the ability of U.S. industry to sell encryption to this global market.

The intent behind export controls was to deny access to encryption both abroad and domestically. Neither the National Security Agency nor the Federal Bureau of Investigation wished to see widespread use of encryption, as this would damage their communications

[2] The most recent expression of this can be found in the 2009 Administration Review of Cybersecurity Policy

intercept capabilities.[3] This put them squarely at odds with American business. Efforts at a compromise, by offering "government friendly" encryption that preserved law enforcement access to communications did not solve the problem, as these products did not appeal to foreign markets. The result of the U.S. controls was to create foreign competitors producing similar products that gobbled market share, rather than to deny other nations access to the controlled technology. Encryption controls were self-defeating, as they created foreign producers who could sell advanced encryption in both the U.S. and other countries.[4]

For the privacy community, the intent of government agencies to deny private citizens the ability to encrypt their messages and to preserve (some would say expand) governmental abilities to intercept communications posed a direct challenge to privacy, civil liberties, and the innovative potential promised by the new technology. The encryption debate expanded mistrust of government – especially since many privacy advocates were convinced that U.S. agencies had built "back doors" into any encryption it could control, to allow easy access. The encryption debate shaped and confirmed an oppositional relationship between the privacy community and the government.[5]

This adversarial relationship is in many ways peculiarly American, reflecting a historic concern to restrain the authority of the sovereign that dates back to the separation of powers built into the U.S. Constitution. The relation between government and citizens or government and industry in other developed nations is less conflictual, reflected in their more accepting attitudes towards government surveillance. The antagonism to government is built into American politics to a degree not found elsewhere. In the U.S., encryption set a course for conflict, but the inclination was already there.

Encryption controls, had they continued, would have protected government capabilities to monitor communications. They would have also damaged the American leadership in information technology, by putting U.S. companies at a disadvantage with their foreign competitors. This economic concern was accompanied, however, by an assertion that encryption controls would damage civil liberties. That communications intercepts lawfully undertaken damage civil liberties makes sense in the context of a decline in legitimacy and trust of government. It only makes sense if we accept that privacy and civil liberties are inextricably linked, and that one cannot exist without the other.

II. Privacy and Civil Liberties

But privacy and civil liberties are not the same, nor are they linked. We can imagine a situation where individuals would have no privacy and yet could have full civil liberties. This experiment is important. As the Internet and associated digital technologies are gradually increasing the amount of information publicly available about individuals, we are moving ineluctably into an

[3] NSA was also deeply concerned that the new internet was fundamentally insecure. One of the motives for the ill-fated "Clipper chip" was to build encryption into the new networks to make them more secure.
[4] The U.S. briefly considered adding import controls on encryption to counter this.
[5] There is no adequate history of the crypto wars, in part because much of the material remains classified. The default account is Steven Levy's Crypto: How the Code Rebels Beat the Government, but it suffers from sourcing limitations.

era of decreased privacy, which makes it important to determine if civil liberties are affected as privacy diminishes. Our future will be one of less privacy, but this need not reduce civil liberties.

The issue of political legitimacy frames assumptions about the linkage between privacy and civil liberties. If the state's authority is not legitimate, it is an opponent rather than a protector of civil liberties. Declining legitimacy combined with a lack of consensus among citizens on social and political norms and values, reinforces the perception that the state is more likely to encroach upon freedom than protect it, and that external, nongovernmental bodies are required to counteract this.

The rise of Non-Governmental Organizations (NGOs) is a symptom of changing political attitudes. The declining legitimacy of formal governments propels private groups to assume functions or provide services where they believe government action is inadequate. NGOs are self-appointed governance bodies whose legitimacy derives from adherence to an ideal or by representing some community that is underrepresented in formal political processes. They are alternate governance structures whose complex relationship with national governments – sometimes competitive, sometimes supportive – reflects the belief that formal government institutions are inadequate.

There is a parallel in a decline of legitimacy to Durkheim's idea of "anomie," which describes the breakdown of social norms and values.[6] Declining legitimacy combined with a lack of consensus on norms and values reinforces the perception that the State as hostile to freedom. Like the separation of powers in the Constitution, this perception is also consistent with a strain in American political tradition that dates back to the revolution, that civil liberties must be protected from government, instead of government being civil liberties' protector.

Key civil liberties – freedom of expression, freedom of assembly– are public functions. Civil liberties provide the ability to speak, publish and assemble and to challenge rulers. Their roots are in pre-industrial societies with much more limited notions of privacy. The intent of civil liberties it to promote free public discourse, engagement among the polity, and allow for challenges to leaders and policies. Civil liberties make unlawful the use by the state of coercive measure designed to block or distort this public discourse. If a state can lawfully engage in coercion against political acts, there are no civil liberties. They exist if a person can freely express opposition to government policies without fear of retribution and even work to displace the existing rulers.[7]

The chief risk to civil liberties lies in the use of coercive acts to suppress them. Privacy, pace the Fourth Amendment, offers only limited protection against coercion. Protection against political coercion comes from some deeper causality based on political norms and culture that explains tolerance and protection of political liberty by the State. The basis for this tolerance of opposition lies in the historical experience of democratic nations, and the development of

[6] Emile Durkheim, Suicide, Free Press, 1951

[7] Asserting that privacy is itself a civil liberty is a somewhat circular contention. That courts have endorsed this idea is not in itself conclusive, as many assertions by courts, even the Supreme Court (such as Dred Scott) have rightly been reconsidered and as new information became available or as attitudes changed.

institutions and norms for dealing with dissent that provide an alternative to coercion. A person who objected to a ruler or policy in the 16th Century was likely to face violence or be imprisoned; there were few other mechanisms for dealing with dissent. By the 18th century, new norms and institutions allowed dissent and the peaceful transfer of power.

There is a simple parallel with the introduction of the printing press, which created new sources of information and challenged existing political models. Books and bibles had been rare, handmade commodities, available only to the elite. With the press, citizens could read the bible and in it, they found no reference to the divine right of kings or to aristocratic hierarchies. The mass produced Bibles were profoundly subversive. The authority and legitimacy of the sovereign came under question and it took decades for new political models that better accommodate the newly empowered citizens. This is rough history, but the internet produces a similar questioning of authority and legitimacy to which governments will need to adjust and accommodate. This process of adjustment to the political effects of the internet is still ongoing.

Democratic societies learned to deal with dissent and disagreement through debate and inclusion in the political process. They do not prohibit alternative points of view or information that contradicts their positions and policies. The reliance on debate and inclusion grows out of the principle that no single party or group has an unchallengeable right to rule, and that governments can be voted from office or otherwise dislodged without violence if interested and sufficiently powerful publics decide this is best.

Authoritarian governments do not have these mechanisms for dealing with dissent. They attempt to repress opposing views. The techniques of physical repression have been refined over decades and have been extended into cyberspace. The state's control of the media and communications reinforces this repression, and it remains an open question as to whether authoritarian governments will succeed in their efforts to control new technologies. Sophisticated authoritarian regimes are adopting tactics that can be termed "selective repression." Politically active individuals are targeted for coercion, while the general population is left unconstrained. The idea is as old as Herodotus, and avoids the resentments created by mass restrictions. Selective repression allows a government to tolerate speech, assembly, religion, travel, gun ownership, even incomplete surveillance as long as the population is politically inactive or passive.

Conversely, societies with strong central governments states and extensive surveillance can respect the civil liberties of their citizens, if they respect freedoms of speech and assembly. [8] No one would say that France and the United Kingdom, for example, are police states where the fundamental right of citizens to engage in politics and change governments, policies and leaders through persuasion and elections, are constrained. Cultural attitudes towards privacy and the role of government differ in these and other countries. Europeans are, if anything, stricter in their protection of individual privacy in commercial activities, but also much more tolerant of government action, including surveillance.[9]

[8]See, for example, The Economist, "The clash of data civilizations," http://www.economist.com/node/16377097

[9] "European attitudes towards surveillance may be indicative of a more balanced and less politicized approach." Benjamin Goold, "Making Sense of Surveillance in Europe," European Journal of Criminology, March 2009

The democratic state is the bulwark of civil liberties. Yet the privacy debate often focuses on the state as the greatest threat. Some of this can be explained by the history of the privacy movement. One of the first privacy organizations, the American Civil Liberties Union (ACLU), was founded in 1917 in opposition to the American entry into World War I and to the draconian measures used by the Federal government against opponents of the war. These opponents included pacifists and isolationists, but they also included a very small number of militant socialists who were not adverse to the use of violence. The ACLU and its founders, Chrystal Eastman and Roger Baldwin, set a precedent linking privacy to "progressive" political causes.[10]

Looking back, we can see that the Justice Department and local officials used the war and the threat of a "red" insurgency as an excuse to suppress political opponents. Free speech was restricted, the most telling example being the jailing of Eugene Debs, the Socialist candidate for President, but this was accompanied by many other acts of official violence against political opponents during the war and for some years afterwards. While a few radicals waged a campaign we would now describe as domestic terrorism, such as exploding a bomb on Wall Street, the overreaction of the political leadership and the blending of business interests and anti-immigrant sentiment was one of those lapses in civil liberties – there have been five since 1917[11] – that occur whenever America faces new, dangerous and unexpected security challenges.

Such outbreaks in American history are likely unavoidable, the result of some central imperfection. There are times when the political leadership will be incapable of policing itself, and non-governmental bodies like the ACLU are essential in mitigating the scope of these outbreaks. Privacy, however, was not the main consideration for this mitigation. Americans enjoyed a much greater degree of privacy in 1919 than they do today, yet their civil liberties were clearly at much greater risk in that era.

Research shows that privacy, in the sense of limiting access to information about an individual, enables independent personal choices that may otherwise be chilled. A person who is being observed, or who believes that he or she is being observed, will often act differently than a person who believes that he or she is unobserved. But linking this loss of privacy and decline in autonomy to a chilling effect on civil liberties rests on a number of assumptions. It assumes that individual attitudes towards privacy remain the same. Individuals who are more comfortable with less privacy may not experience the same chilling effect. It assumes that the increased ability for communication and publication provided by the Internet does not offset the potential loss of autonomy. A more extroverted society will not experience a chilling political effect.

Less privacy does not automatically lead to less political freedom and fewer civil liberties if free

---

[10] "Throughout the 1920s labor and political speech issues predominated [in the ACLU]. The organization remained silent on such issues as the Volstead Act, the Olmstead wiretapping case, and other due process or privacy law questions." http://diglib.princeton.edu/ead/pdf?id=ark:/88435/rj430454b

[11] The Red Scare of the 1920s, the 1941 internment of Japanese-Americans, the 1950s McCarthy /House Un-American activities; the surveillance of the 1960s and 1970s, including Watergate; the Post 9/11 actions to monitor for terrorist activities.

,[12] To take a recent example, the actions of the Bush Administration's warrantless surveillance program raised serious concerns, but had no effect in reducing political debate over the administration's policies, as it was not used for domestic political purposes.

speech and freedom of assembly are protected.[12] This suggests the best protections for civil liberties are to avoid regulating content,[13] and, as it becomes increasingly easy to obtain personal information, to expand transparency in governmental activities and place clear limitations on the use of information government or companies collect. With these in place, if free speech and freedom of assembly are protected, less privacy will not lead to decreased political freedom and civil liberties in democratic states.[14]

III. Anonymity and Civil Liberties

If the state is a threat, hiding from it is essential. The internet makes it easy to hide. It was not designed to provide strong authentication of identity. This lapse is the result of a close focus on the imperatives of building strong connectivity and because no one expected this technology to become a world circling infrastructure used by hundreds of millions. The internet lets one assert any identity online, including a null assertion or anonymity. Anonymity is the inescapable "default position" on the internet, and this is damaging.

The opposite, an ability to identify completely each individual also holds some risk, but the risks to civil liberties in a democratic nation are overstated. In the absence of adequate privacy safeguards, anonymity is an important protection for consumers. It is reasonable, for example, to want to deny your insurance company the chance to find out what health websites you visit, as they may use this against you. Many in the privacy community believe that anonymity is also essential for civil liberties. The examples given are always a human rights activist in Central America or a dissident in China. They are not drawn from western democracies. Of course, some of the more extreme privacy advocates would argue that democracies like the U.S. or those in Western Europe are charades. Others believe that governments constantly seek to increase the power of the police, and major privacy organizations in the United States fear that "we are constructing a national surveillance state."[15]

We know what surveillance states look like. Their most prominent feature is a massive domestic security apparatus, employing tens of thousands of people. STASI, the East German Security Agency, had more than twice as many employees as the FBI does now, for a population that was one twentieth the size of the United States – the FBI would have to be expanded forty fold to match STASI. Domestic security agencies in surveillance states are excused from observing most laws and have broad authority to arrest or detain for political reasons rather then criminal acts. Extensive monitoring of domestic communications for political purposes is routine, and most "surveillance states" employ thousands of local informants. The most advanced agencies also use sophisticated computer programs to collate deep personal information.[16] All of these powers are gathered in a single agency that reports directly to the political leadership, without any external oversight. There are no "surveillance states" among the western democracies. A

[13] U.S. and European democracies differ on control of content Europeans restricts 'hate speech." They would assert that their restrictions are bounded by the need to show an imminent risk of harm, which minimizes the effect on civil liberties. Restrictions on hate speech were an important complication in negotiating the Council of Europe Cybercrime convention.

[14] Assuring transparency will require the creator of new oversight bodies within government and a more active role by the Congress.

[15] EPIC, 2007 Annual Report, http://epic.org/epic/annual_reports/2007.pdf

[16] Similar to that collected by data aggregators in the U.S.

close examination of policy and spending would show that the fear of a surveillance state in the United States is a wild exaggeration, perhaps reflecting the eroding legitimacy of Federal institutions, but this belief reflects helps explain some of the desire to protect anonymity.

Anonymity as a virtue reflects the ideology of the internet pioneers that government threatens rights rather than protect them and that anonymity is essential for the exercise of freedom of speech. In non-democratic states, where speech is suppressed, anonymous statements may provide some degree of political liberty if the security services are lethargic or unsophisticated. Aggressive security services can manage the challenge of anonymous communications. Anonymity, in a country that provides for freedom of speech, can have an anti-democratic effect. The effect of anonymity in democratic states can be to cut the link between citizen and personal responsibility, damaging the essential communal nature of politics. Anonymity can allow the expression of opinions without fear of retaliation, such as an employee revealing misdeeds by an employer. In a country that provides freedom of speech, it can also undermine the legitimacy of democratic institutions and, as a result, weaken the protections they provide for civil liberties.

The internet and its new technologies create a complex political environment. It provides new ways for individuals to identify with groups and to attach loyalty. It disconnects public discussion from physical location, and may increase the risk that community will increasingly be defined as those who think like us rather than those with whom we share a space. Before the internet, a person with extreme views may have been isolated in their community. Now, they can go online and find that there are thousands who share their beliefs. They can organize and recruit. This may be only a temporary phenomenon, as democratic political systems adjust to the widening of participation in political life.

The pioneers of the internet believed it would be a democratizing force. John Perry Barlow put is this way: "The Net is about taking power away from institutions and giving it to individuals."[17]
The pioneers were right, if by democracy we mean greater participation in the political process. The effect of the new technologies is not democratic in the sense of an endorsement of western values, including freedom of expression and assembly. Over the long term – perhaps decades - greater access to information and greater participation will expand democracy, but the immediate political effect of the internet has been to resurrect, expand and energize extremist views.[18] Access to the internet reinforces existing political trends, favorable and unfavorable. When certain conditions are present – simmering discontent, a triggering incident and, perhaps, charismatic opposition leaders – the new technologies and the internet provide a tool for strengthening this opposition and for more easily coalescing discontent into action. Absent these conditions, however, the political and 'democratizing" effect is limited, and we want to avoid overstating the causal role of the new technologies in places like Egypt, Tunisia or Libya.

---

[17] See, for example, "Wizards, Bureaucrats, Warriors & Hackers: Writing the History of the Internet," Roy Rosenzweig, *American Historical Review*, (December 1998); John Markoff, What the Dormouse Said; Turner, From Counterculture to Cyber Culture; "Daily Life in Cyberspace: How the Computerized Counterculture Built a New Kind of Place;" Out of Control: The New Biology of Machines, Social Systems, and the Economic World (1994)
[18] For a brief discussion, see Michael Barkun, Conspiracy Theories in Politics, New York Times, April 22, 2011, http://www.nytimes.com/roomfordebate/2011/04/21/barack-obama-and-the-psychology-of-the-birther-myth/conspiracy-theories-in-politics

One way to approach the issue is to ask, if there were no anonymity, would American politics be noticeably different? Anonymous contributions to the political debate are scarce. While press accounts may quote anonymous sources, the reporter or editor usually knows the identities of these sources. Standing for office requires strong authentication of identity. Democracies enfranchise participation in the political process to all eligible residents of a region (although the conditions of eligibility have been a longstanding source of contention) through a process of enrolment and identification. It is important for ballots to be anonymous, to prevent coercion, but it is equally important for eligibility to vote to be fully authenticated, to prevent fraud. A public discussion or debate may allow an individual to question or shout comments without identifying themselves, but their physical attributes are not concealed and they are often known to members of the audience. Anonymity may give voice to the powerless, but in democratic societies, it can also corrode an essential trust.

A conversation with members of the group "Anonymous," who launched annoying revenge exploits against the public websites of companies that had taken action against wikileaks, highlight the weaknesses of anonymity. These individuals compared their actions to the civil right protestors in Selma and the Greensboro sit-ins. But the protestors in Selma and Greensboro were not anonymous. They did not hide. Their actions were heroic and it was this heroic confrontation that had political effect. In contrast, the effect of the anonymous wikileaks "paybacks" was ephemeral.[19]

The companion of anonymity, weak authentication of identity, is of course also a key enabler of cybercrime. Better authentication of online identity could improve cybersecurity (although we do not want to exaggerate the scope of any improvement). The more important issue is that anonymity creates a lack of trust, which is among the Internet's biggest problems. The lack of trust hampers the growth of new internet applications that offer new services and new savings. A complete lack of anonymity conjures up images of an Orwellian police state. Complete anonymity in turn, produces a Hobbesian state of nature. Neither extreme is preferable. Our current situation, reflecting the proclivities and assumptions of the internet pioneers, is closer to the latter than may best serve the public interest. This is a complex and emotional subject. Law and social practice will need to adjust to the potential for anonymity provided by the internet, and this will require norms, rules and technologies that preserve anonymity in some areas and constrain it in others, rather than making it the default option for the internet.

IV. Preserving the Open Internet to Promote Innovation

Privacy advocates oppose some cybersecurity measures because they threaten the open internet and innovation. We could again undertake our experiment of asking what effect a complete absence of privacy would have on an economy that observed the rule of law and had strong protections for intellectual property. The deciding factors, this experiment suggests, is an ability restrict the temptation for existing businesses to block innovations that could threaten their profitability and to protect innovators and entrepreneurs from the theft of their new ideas. If incumbent power were restrained and intellectual property protected, innovation would continue irrespective of the status of privacy or internet freedom.

[19] NPR, "'Operation Payback' Targets WikiLeaks' Foes," http://www.npr.org/2010/12/09/131937254/-operation-payback-targets-wikileaks-foes

Yet, one leading privacy organization states that it "strongly believes that [privacy] is essential to keep the internet open, innovative and free."[20] The belief that a "free and open" internet is linked to innovation deserves greater attention, but some discussion is necessary as the belief forms an important element of the rationale for blocking cybersecurity initiatives if these involve a larger role for government (rather than individual, voluntary actions).

The role of the privacy community in the dispute over net neutrality helps to illustrate this point. Net neutrality, the idea that service providers should not be able to limit access to content or create tiered levels of service and that all traffic should be treated equally, has little to do with the protection of personal information, yet every major privacy organization supported it as essential for preserving the open environment needed for innovation. Privacy's economic agenda seeks to preserve the internet in its unconstrained, pioneering state as a driver for economic growth.

Privacy and economics overlap in three ways. First, the new technologies lead entrepreneurs to find new ways to take advantage of networked technologies, by collecting information on consumer preferences and habits, often without the consumers' knowledge or consent. The amount of information generated by the internet on consumers is unprecedented, and the technologies developed to collect this information usually falls outside the ambit of existing law. This is a particularly important problem for the United States, where the laws regarding such collection and exploitation activities by businesses are weak. Here, innovation unconstrained by law is antithetical to privacy.

Second, the disruptions created by the new technologies prompts companies to defend existing business models by using law and regulation to limit competition. This is particularly true in telecommunications and broadcast industries, where incumbents and existing companies often exercise extensive power to safeguard their interests. The relationship between the privacy community and business involves a degree of discomfort. There is an affinity between privacy advocates and the "new" tech companies who threaten the old giants. The efforts of incumbents to protect intellectual property or create new revenues streams by exploiting consumer information usually run afoul of privacy. At the same time, the privacy community's advocacy of a free internet and limited role for government attracts support from business interests that seeks to limit regulation and liability. The argument that the internet must remain free to empower innovation has become a useful blocking tool in policy debates and in Congress.

Third, the internet is seen as a wellspring of innovation. This is probably reflects a misunderstanding of the innovation process. Innovation, the creation of new ideas, services and technologies, allows economies to grow and use resources more efficiently. Recognition of the importance of innovation grows out of a long sequence of work in economic theory. Schumpeter and other late 19th century economists identified innovation and entrepreneurship as essential economic factors. Twentieth century economics like Robert Solow, Kenneth Arrow, and others, demonstrated that technological innovation is the key determinant of growth.

Digital technologies now drive growth. The issues for consideration are the rate of that growth

[20] Center for Democracy and Technology, http://www.cdt.org/about

and the policies that best accelerate it. The expanded production of digital technologies (such as computers) has been a source of economic growth as the IT manufacturing sector expanded to meet demand, and as companies outside of the IT sector used digital technologies to become more efficient. Digital technologies allowed the creation of new network services. While the first two elements – IT production and increased efficiency in non-IT industries - are more important in explaining economic growth, the latter element – e-commerce and the creation of new, mass-market network services – has come to represent digital innovation.

Some economists at first believed that the contribution of digital technologies was entirely overstated. As more data became available, the contribution to growth became clearer. In combination, the expanded production and increased efficiency probably accounted for a third of U.S. productivity growth in the late 1990s.[21] But growth did not increase at a constant rate. Companies outside of the IT sector reaped the largest efficiency gains early on; the rate of increase in improvement gains for these companies is now smaller. Economists would be familiar with this as the concept of diminishing marginal returns.

In contrast to the initial skepticism of economists, advocates of the new technology concluded in the 1990s that we were entering a "new economy," where a "technology fueled productivity boom" would eliminate business cycles and recession. The notion of permanent growth had appeared in the stock market bubble in the late 1920s, which, like the new economy of the 1990s, was fueled by lax monetary policy, rather than some underlying and permanent change. The commitment to a free internet as a source of growth retains a tinge of this dot-com era belief in a "new economy" where constraints on growth had been eliminated by information technology.[22]

Any discussion of the economic effects of the internet and digital technology is necessarily complicated by the larger problems in measuring and explaining growth and innovation. Innovation involves many factors. Access to information technology is one factor, but not the most important. An educated workforce, appropriate fiscal and tax policies that create the financial resources needed for investment, balanced protection of intellectual property rights, and minimal regulatory impediments (at all levels of government) are key, along with adequate infrastructures, and openness to trade. Progress in these areas is necessary to increase innovation, but each may require difficult political decisions that go well beyond a commitment to preserving an open internet.

Open platforms encourage innovation in some areas, but that does not mean that innovation and growth would cease or slow if the open platform was unavailable. Robert Fogel's point, first raised in his landmark study of how a new "networking" technology affected American growth in the 19th century,[23] is that the actual contribution to economic growth of a new technology is determined by asking what growth would have been if the new technology had never been

[21] Robert Solow, who famously said in 1987 "You can see the computer age everywhere but in the productivity statistics." Stephen Oliner and Daniel Sichel, "Information technology and productivity: where are we now and where are we going?" FRB, 2000; Kevin Stiroh, What Drives Productivity Growth; Gordon; Litan and Rivlin, "Projecting the Economic Impact of the Internet,"

[22] See, for example, Jennifer Rheingold, "What We Learned in the New Economy," Fast Company, http://www.fastcompany.com/magazine/80/neweconomy.html?page=0%2C1; Alan S. Blinder, Brookings, The Internet and the New Economy," http://www.brookings.edu/comm/policybriefs/pb60.pdf

[23] Robert Fogel, Railroads and American Economic Growth: Essays in Econometric History, 1964

invented. For other major innovations, the rate of change is incremental, not revolutionary. We need to be cautious in ascribing a broad range of economic virtues to a single technology if we are to avoid damaging missteps that impede both growth and security.

That an open and free internet is essential for innovation has become a defining myth and reinforces arguments that the internet must remain unregulated and the role of governments constrained. But there is more to innovation than creating a new app or social network site. The most telling evidence against the link between an open internet, innovation and growth lies in Asia,[24] where nations with much less privacy and very different conceptions of it are moving to displace the United States as the leading global innovator. They have already displaced Europe. The best explanation for this tectonic shift is that privacy is irrelevant to innovation.

IV. Futures for Privacy

The technological and social context for privacy and internet governance is not static, and further changes will reshape privacy. The new ways in which people connect to the global network will affect privacy. The old hobbyist model of computing, where personal data was stored on a box next to your desk is being replaced by technologies where data and applications are stored and managed remotely. The ability to exploit information gleaned from an individual's web activities is growing. Access to and control of personal data will be shared, controlled by third parties and governed by laws and contracts that are often inadequate.

We can find a precedent for this transition in the history of other utilities. For a brief period at the start of the electrical age, people who wanted electricity had to provide it themselves, using generators in basements or carriage houses. They had to maintain the machinery, upgrade it, and worry about safety. Sometimes they sold power to their neighbors, creating local networks. This was neither efficient nor safe. People now buy electricity as a service without any knowledge or concern as to where the power is being generated or by whom, but the provision of this service is highly regulated to protect the public. A similar transition is occurring with the internet. The move from disaggregation to the cloud changes the relationship between privacy and cybersecurity. In this cloud-computing environment, we will rely on third parties for essential computing and network services, and as a result, third parties will play the central role in cybersecurity.

This is a significant departure from the past, where each enterprise, agency or user was responsible for their own data and its defense. The internet was designed to put responsibility for all but the simplest addressing functions, including security, at the devices at its end points. The advantage of this disaggregated approach to security is that it minimized political problems that revolve around the role of government in supplying a public good – there is less need for regulation and there is an implicit protection for privacy as third parties are not involved. The disadvantage, of course, is that even an unskilled opponent can easily defeat a disaggregated defense.

[24] China, a country that has infinitely less internet freedom than the United States, grows four times as fast and threatens, if the American scientific community can be believed, to overtake us in technology and engineering. China's example suggests that close attention to fiscal and economic fundamentals are more important for growth than a free and open internet.

DHS's Einstein programs point to the future, where cybersecurity functions will be automated across networks. These new approaches, called "active defense" or "dynamic defense," monitor traffic for known malware and, in some cases, for anomalous activity. These systems take action to block such traffic before it can penetrate the network being protected. Once problematic traffic is identified, dynamic defense systems use pre-programmed decisions that tell the system what action to take when it identifies a particular signature or class of signatures as malicious. Dynamic defense parallels "Network-centric warfare," with its emphasis on networks rather than platforms, information-sharing to increase situational awareness, and speed.

However, these dynamic techniques are intrusive and can require a high level of monitoring. To be maximally effective, they need to be informed by intelligence data and by combining traffic data from multiple service providers. The combination of monitoring, speed and intelligence involved in a dynamic approach to cybersecurity, whether it is for government networks or some broader set of infrastructures, create immense problems for the privacy community. We can legitimately ask, however, whether monitoring that is limited to identifying malware and does not produce new information or knowledge on the content of traffic for government use that is carried out by machines without human intervention, poses any risk to civil liberties.

One response to this change has been to assert that dynamic defense does not actually work. This is a rhetorical device – to object to technologies on the grounds that they are ineffective. The problem is that these charges are often divorced from data. We now have the capability to count and measure the effectiveness of techniques and technologies in blocking attacks and mitigating risk. The data suggests that active, networked defense is more effective than a disaggregated, point defense. Interviews with leading network service providers who use these technologies on their own networks to protect their customers and service suggest that active defense is a significant improvement.

Given the potential intrusiveness of active defense, strengthened oversight procedures and limitations on the use personal data are essential. The challenge for the privacy community is to find way to help provide new rules oversight without blocking the use of the new defensive technologies. Doing this will require moving away from the ideological precepts of the internet pioneers and becoming partners in deployment rather than opponents of technological change.

Attitudinal changes among the electorate towards privacy also need closer examination. One challenge for privacy organizations is that the political impulse that led to their creation may be fading because of generational change. There is less privacy now than in pre-internet days, but that people are more willing to share personal information does not mean they are then willing to have that information collected or used without their consent. The decline in privacy is in part a result of technologies that make it easier to publish, find and access information, and in part a matter of personal choice, as people choose to publish more personal information (perhaps in some cases without realizing that they have made it public).

While we do not want to overstate "the end of privacy" or a generational shift in attitudes on sharing personal information on strangers, network technologies enable greater access and sharing. What we may be seeing is the effect of a change in the economics of sharing. People

did not share personal data widely before the internet; we assumed this reflected a preference. An alternative explanation is that they did not care if information was shared, but were unwilling to pay the price in time and money to do so. Their attitude has remained the same – they do not care – but the internet has lowered the price of sharing and access. Attitudes towards privacy will change because of lower costs, and the urban individualism of the industrial age, the ideal of pre-digital privacy – is gone forever.

Privacy is shrinking as the world becomes interconnected. The increased incomes of the 19th and 20th centuries allowed people to occupy greater personal space instead of the crowded and close villages and towns of an earlier era, where there were far fewer secrets. The growth of transportation technologies increased the opportunity for anonymity (or pseudonymity) by allowing an individual to rapidly relocate to a place where he or she was a stranger. The internet, by eliminating physical constraints, undermines this old-style privacy. As privacy changes, the expectations of the internet pioneers and the policies that append from them will also be undermined. In the future, as personal data becomes increasingly ubiquitous, privacy may need to enable greater individual control over the use of data rather than seeking to preventing its discovery.

V. Internet Governance and the Closing of the Electronic Frontier

It is reasonable to ask if concern about government cybersecurity programs would decrease if the U.S. had a comprehensive set of protections for privacy in commercial activities. The likely answer would be that this would not greatly change privacy views of better cybersecurity. Concerns over the role of government would remain, as would the imperative of preserving the internet's open frontier so cherished by its creators.

The question we have been reluctant to ask is whether the beliefs of the early 1990s, when the internet was smaller, largely American and not a global infrastructure, are still adequate and retain persuasive force in the changed international environment. U.S. policy was seminal in shaping internet governance and the visions of the internet pioneers shaped this policy. In turn, this vision and policies shaped how the world perceived the internet. U.S. policy was seminal in shaping internet governance and the visions of the internet pioneers shaped this policy. In turn, this vision and policies shaped how the world perceived the internet. The decision of the United States to take a minimalist approach to regulating the Internet initially had considerable influence on other nations. In part, this reflects U.S. efforts in multilateral fora like the OECD and UNCITRAL, where the U.S. led efforts to adopt policies that emphasized private sector control. The American origins of the new technology and the rapid growth of the American economy in the 1990s made other countries more accepting of this leadership.

For reasons both good and bad that intellectual construct is now collapsing. It is inadequate to the tasks of managing the new technology and this inadequacy reinforces the growing tendency of other nations to question the old dogma and undertake efforts to restructure internet governance. Since 2006, the failure in Iraq and the general attribution of the global financial panic to American irresponsibility has tarnished the luster and reduced the influence of the United States. Challenge by new economic powers was inevitable, but we are in a weaker position to respond to it, and this poses a risk to democratic values.

We are in a transition to a new kind of internet governance. Two related trends drive this transition – the extension of sovereign control into cyberspace and the collapse of the pioneering, communal, American vision for governance. Managing this transition in a way that preserves the values free speech and open access to information will be difficult. Continued espousal of the pioneering concepts will keep the U.S. on the defensive, as it tries to preserve an increasingly inadequate internet governance model, and may even condemn the U.S. to irrelevance, as other nations move to new approaches where governments play the same role in cyberspace that they play in other multilateral activities. A strategic approach to cybersecurity, and a framework for privacy suited to the new social and technological environment, requires new ways of thinking.

The view that the internet must remain "free" and an open frontier is a serious impediment for taking full advantage of network technologies. There will be unhappiness as governments move to play a stronger role in protecting the internet frontier, and these efforts will be cast as a threat to civil liberties and the economy. But it is time to extend the rule of law into cyberspace and abandon the pioneering concepts that shape internet governance and privacy policy. They no longer make sense for a global network where there are increasing challenges to security and to the values of openness, free access to information, and free speech. To do this, conceptions of privacy and its connection to civil liberties and innovation must be refocused and renewed.

The global governance debate revolves around the issues of sovereign control over access to information and the role of the state. One possible outcome of this debate is a slow fragmentation of the internet into linguistic and regional blocs, which authoritarian governments will shape to serve their needs. This outcome is not in the U.S. interest, nor in the interest of the world, but if the U.S. cannot offer some new conceptual framework that escapes our pioneering vision of internet governance, it is the most likely.

While there is no global consensus on privacy, just as there is no global consensus on free speech, the one area where citizens in most countries agree is that they should have untrammeled access to information,[25] and that access to information should be a new fundamental human right. Not all governments share this belief, but it offers an opportunity to build a new consensus on internet governance, security and civil liberties based on expanding access to information. Otherwise, a more fractured Internet may emerge, with privacy protected for some and fewer civil liberties for many others.

The U.S. is unaccustomed to seeing major international initiatives undertaken without its leadership, but this is what is happening because of an American inability to move past the internet's pioneering ideology. The pioneering framework is broken; it failed to provide security and did not meet the needs of many nations. It incapable of guiding policies that make the internet more secure. The long and sustained political effort in the U.S. to attack and diminish the role of government and the private sector as an alternate governance structure "private enterprise as a form of voluntary social cooperation undergirding strong communities and democratic self-government"[26] is alien to other nations and makes U.S. public policy debates markedly different from that in other nations. The pioneering internet notion of private sector

[25] BBC, "Internet access is 'a fundamental right" http://news.bbc.co.uk/2/hi/technology/8548190.stm
[26] American Enterprise Institute, "History of AEI," http://www.aei.org/history

lead and small government role is also alien to these nations.

The current structure of Internet governance grows from uniquely American cultural and political roots. The internet is the product of the times, and much of its governance structure is a legacy of the politics of earlier eras. Predictions about the demise of the nation-state and the emergence of a "borderless world" were a regular feature of discussions of international relations in the 1990s and helped shape views on internet governance. They have now become somewhat muted, as these predictions overstated the effects of globalization and did not take into account the ability of nation states to adjust to the new circumstances.[27] The internet did not eliminate borders; it shrank the time to traverse geographic space. It did not replace governments with a self-governing global commons shaped by private action, where formal state mechanisms were unneeded. Governments will adapt to the new technology and nation-states will remain the most powerful actor on the global stage and assert themselves in cyberspace. As governments reassert themselves in cyberspace and develop ways to "strengthen" borders, those who continue to espouse the pioneering ideology risk being condemned to irrelevance.

The next few years will see governments extend sovereign control into cyberspace. They have realized that the notion that the cyber domain is somehow outside the realm of sovereign control is inaccurate and does not reflect how networks are constructed and operated. In light of this, a reassessment of internet governance is essential. For privacy policy, this reassessment would ask how it would be different if the pioneering internet ideology were no longer its foundation. The most likely changes would be an end to the belief that a completely open and free internet is necessary for innovation, and that the role of the state in cyberspace should be smaller than it is for any other social or economic activity. A more difficult reassessment would look at the changes in attitudes towards privacy, particularly generational changes.

Any process of reconceptualization will be difficult. Thomas Kuhn, in a seminal study of how scientific concepts change, noted that new ideas persuade adherents of the old to change their minds, it is that the believers in the older concept eventually die and are replaced by those with new thoughts.[28] This gloomy prognosis is not entirely appropriate for the Internet. There is no guarantee that the United States will adopt this new mindset, but there are some reasons for hope. Until recently, debate over Internet policy was largely confined to specialists, often from a technical background or from the IT industry. They were largely American, with views shaped by the American political experience. Now that the Internet has become a central element of daily life, new interest groups and countries with different political views will become involved in these debates, which will dilute the influence and question the beliefs of this older community. The challenge for the United States will be to manage this transition so as to not lose the virtues of American ideology – the commitment to openness and individual freedom – while moving to mature governance for the new global infrastructure.

[27] Kenneth Waltz, "Globalization and Governance," *PS Online*, December 1999, http://www.mtholyoke.edu/acad/intrel/walglob.htm

[28] Thomas Kuhn, The Structure of Scientific Revolutions, 1962