The Public Record:
The State, Security and Lessons From Participatory Culture

William Uricchio
MIT and Utrecht University

The tragic events of September 11, 2001 seem like a turning point in American culture, marking a transformation from what in retrospect seems like an innocent age, to an era marked by fear, isolation, and demagoguery. From a prosperous land with little more to preoccupy it than the sexual foibles of its president, the United States found itself transformed into a debt-ridden nation in a state of war both internally, over domestic values, and externally, with an elusive and invisible enemy. From an open country enjoying good relations with its allies and meriting respect thanks to its support of humanitarian and environmental causes, the US embarked on a self-styled "crusade" grounded in moral righteousness and military might. The starkness of the situation found expression in President Bush's battle cry of "with us or with the terrorists," a polarizing discourse that sustained pointed incursions into the nation's founding values as evidenced by the terms of the "Patriot" Act and the treatment of foreign nationals in Guantanamo Bay. In the struggle to balance the openness and liberties so central to America's identity against the need for security and defense provoked by a faceless and transnational enemy, many conflicting opinions were voiced.

In the pages ahead, I would like to pursue this moment and the evident crisis it provoked in the relationship between the state and security. Post facto assessments of the events of 9/11 were strongly divided: was the attack provoked by envy or hatred of America's 'success'? Were the terrorists aided in their acts by the nation's 'abundance of freedom' and open information? Or were they enabled by poor information flow, administrative complexity and communication breakdowns? These assessments would be determining for how the nation reflected upon its security needs, and for the actions that would follow – both in terms of domestic and foreign policy. The events of 9/11 raise a series of crucial questions regarding the state and security, questions – I will argue – that go beyond the predictable concerns of protecting the nation from terrorist attacks. The relationship between the state and security, as this volume demonstrates, is complex, and while we normally look to the state for security against terror and a host of other concerns, I would like to consider what happens when a duly elected government *itself* poses a threat to the security of its people, the nation's constitutional framework, and the fabric of the state itself. Such an argument requires disentangling national security from the state, something that can only be done through a heuristic move that understands the state not as an abstract category but rather as a set of embodied practices. It requires embarking onto an admittedly slippery slope between the state as a transcendent principle, and the state as it is deployed and materially manifest. The term 'government' and the processes of governmentality are generally invoked for this more pragmatic manifestation of the state-in-action at a particular historical juncture. However, one of the complications of the post 9/11 turn is that the government, an entity characterized by its ephemeral partisan embodiment, has sought to cloak its activities with the more transcendent authority of the state, on whose behalf

it operates and is empowered to administrate.[1] This slippage can be read in many ways: from the government's reaction to perceived crisis and the need to consolidate its activities under the banner of the state, to a cynical attempt of some within the government to seize power and in the process, redefine the state in an extra-legal manner. It is not my point in this chapter to characterize the motives behind recent developments, so much as to use these developments as a means to interrogate a reciprocal to the more familiar invocation of the state as guarantor of security against terrorism: how do we protect the security of the state – and its people -- against its own instruments of governmentality? How can we maintain the integrity and security of the state from internal threats, in addition to those more easily defined as external and terroristic? To answer these questions, I would like to focus on the topic of information flow, arguing that it is essential to the transparency – and evaluation -- of government in a democracy, and therefore to the health of the state. If the flow of information is stopped, the government is effectively free from public scrutiny. Such freedom comes at a potentially high price, permitting easy slippage between partisan interests and the interests of the state, undermining constitutional frameworks, and doing all of this without consequence. The viability of the state hangs in the balance. The irony of the current moment is that security – as a means of protecting the state, its territories and peoples, from terror – is the very instrument that is being deployed to subvert the state from within.

The current US example of the concentration of state power by a partisan cohort is complicated by three coincident large-scale developments: increased concentration of the international media industry; the extensive growth of surveillance technologies and data-mining techniques; and the rapid uptake of distributed, networked and peer-to-peer communication. These developments have variously enabled the quick transformation of political realities (concentrated media), offered opportunities for far more egregious extensions of the current logic of control and incursion into traditional state-protected freedoms (pervasive surveillance systems), and provided channels for popular resistance (distributed networks). My argument will link media concentration to the decline in pluralism and the demise of a culture of public debate that typified the post-9/11 American scene; sketch the dilemma posed by contemporary surveillance practices, and suggest that the new, distributed media offer ways of securing information and access that can enhance the security of the state both from forces of terror and from governmental misuse.

Three preliminary notes are necessary. First, although this chapter draws on examples from America and from trans-national developments in Internet culture, the dynamics it sketches are relevant for Western states generally, and particularly those with such tell-tale signs as governmental failures to share information with citizens regarding such 'sensitive' activities as participating in extraordinary renditions, secret imprisonments, and illegal surveillance.[2] Even if pressured by or tolerated on the behalf allies, such transgressions erode and even subvert the responsibilities to the state of elected officials. A second point regards the word *security* in the English language. Although the word first appeared ca. 1430 (meaning 'protected from danger' soon followed by 'anxiety' or 'care'; and 'means of payment'), the extension of security to state affairs took place much later, during the Second World War ('the safety or safeguarding of a state against danger'). Related spin-offs such as 'security services,' 'security clearance,' 'security act,' "security risk,' etc. tend to be even more recent, for the most part emerging in the 1960s and 1970s.[3] The relatively recent timing of these

state-related meanings reveals something about the term's conceptual framing, indicating among other things that it was not triggered by the emergence of the modern state. Rather, first deployed in English with regard to the state in 1941, the term coincides with the appearance in public discourse of the military-industrial complex, and pointedly addresses an awareness of new vulnerabilities to the fabric of the state from within, such as espionage and subversion, above and beyond the age-old concern with the external dangers of war. The Cold War sustained this focus on state security as concerning internal threats of subversion, underscoring my argument of continuing to consider internal threats rather than only considering external forms of terrorism. Third, although I will be advocating maximum transparency and availability of information as a way of securing the state, I understand that there are exceptional cases (advanced weapon design, for example) where information must be restricted to a 'need to know basis.' I understand openness as a default option, and any departures from it to be extraordinary, well-grounded, and open to oversight and debate.

A state of insecurity?

Somehow, despite the fact that nearly a third of the September 11 victims were "foreigners," or that the goal of the terrorist attack was the *World* Trade Center, or that the community of nations demonstrated an unparalleled level of sympathy and support, the attacks were framed as an assault upon *American* values and ideology. The US's recently elected political leadership was quick to narrow the meanings of the attack, re-defining the historical role of the Bush presidency and its grip on state power. Rather than engaging in reflection, debate, or nuanced analysis, large sectors of the American media appeared to address these developments through a growing dependence on national symbols, invoking the icons of flag and president, and the endlessly reiterated images of the collapse of the twin towers. Understood as symbols of national unity by some, God-given righteousness by others, and imperialistic oppression by yet others, the use of such polysemic images both benefited -- and suffered -- from an inherent ambivalence. The media coverage of September 11 and its aftermath, including the wars on "terror" and the territories of Afghanistan and Iraq, seemed to mark a shift from the discourse of reason to the discourse of branding, the realm of floating signification with all of its evocative yet elusive meanings. Although the potentially reflexive question "why do they hate us" was frequently posed, it was rarely answered with anything other than a re-assertion of nation and might. Meanwhile, many Europeans and particularly the European media struggled to make sense not only of the change in America's emotional tenor, but of the apparent change in its dominant communication strategies.

The meta-narrative of good versus evil that helped to mute reasoned debate over the events of 9/11 has long been a part of Western culture, and has gotten plenty of exposure thanks to the joint efforts of the politically-engaged fundamentalist clergy and religiously-inclined opportunistic politicians. But the turn to such meta-narratives over reason also permitted quick erosion of state attributes that have been in place at least since the Enlightenment (and in the case of the Bush administration's attack on *habeas corpus*, as far back as the *Magna Carta* of 1215[4]). But a more recent and structurally resonant precedent prepared the way for the dynamic of fear of an unseen enemy and the merits of moral righteousness and absolutism as a best defense: the Cold War. And as the recent history of the word *security* suggests, the perceived dangers to the state from Communist subversion were themselves part of a new dynamic. The

paranoia rampant in the period led some government officials to invoke state power in highly inappropriate ways, from unauthorized surveillance to the termination of political freedom to the execution of people based on secret evidence. Fear of leftist state infiltration led some right-wing government officials to preemptive acts of state subversion. In a certain sense, one can see the current struggle over terrorism as drawing its discursive power from the well-rehearsed logics of "us versus them," of order versus barbaric ruthlessness, of the deep seated fear of an ideological other who may well be in our midst, all encouraging the actions of some within the government to preemptively seize the state in the interests of protecting it. With just over a decade of relief from the master narrative of anxiety, the events of 9/11 drew more than a small portion of their intensity – and their logics of response -- from these deeply rooted structures. Seen from this perspective, the responses to the events of September 11th mark not so much a turning point as a continuation of a deeply defined cultural logic. Let's look briefly at the nature of some of the government's responses.

State security at risk: three scenarios

> According to *The New York Times*,
>
> > Thomas H. Kean, chairman of the Sept. 11 commission and a former Republican governor of New Jersey, said the failure to prevent the 2001 attacks was rooted not in leaks of sensitive information but in the barriers to sharing information between agencies and with the public. "You'd just be amazed at the kind of information that's classified - everyday information, things we all know from the newspaper," Mr. Kean said. "We're better off with openness. The best ally we have in protecting ourselves against terrorism is an informed public."[5]

The *Times* went on to reveal cases of "secrecy running amok" including the withholding of the CIA's budgets from the 1950's and 60's; the Defense Intelligence Agency's suppression of the fact that Augusto Pinochet was interested in "fencing, boxing and horseback riding"; the Justice Department's insistence on blacking out a four-line quotation of a published Supreme Court decision: and material that could be found on the very pages of the *Times* itself. According to the Federal Information Security Oversight Office, a record 15.6 million documents were classified as secret in 2004, nearly double the number in 2001, which in turn was significantly higher than 2000. Meanwhile, the declassification process slowed from 204 million pages in 1997 to just 28 million pages in 2004. Kean's assessment of this changed information climate is particularly troubling given that, as committee chair, he was one of the few to have access to secret documents surrounding the events of September 11, the incident retrospectively used to intensify the cult of secrecy in the name of national security. But the widespread and often gratuitous extension of secrecy classification is only one of several techniques that the government deployed.

The Bush administration has also invoked the so called "state secrets privilege" in a series of legal precedents, allowing the government to seek dismissal of lawsuits and cases it said would threaten national security. This effectively allowed the administration to sidestep any challenges to excessive classification, and to not only exempt itself from liability in cases where basic freedoms had been transgressed, but to keep such issues out of the public's eye. Critics contend that this privilege was used to hide embarrassing

information, such as the details behind the president's decision to order the National Security Agency to eavesdrop on overseas telephone calls.[6] Indeed, the precise number of times that this privilege has been invoked is itself unclear since information regarding it is also secret; but based on known instances, the Bush administration has used it more than any other administration in American history. Add to this secret courts (all records are secret, as are the sources of testimony, the names of judges, and the very existence of a trial), secret imprisonments, and constraints on press reports regarding these activities, and the threats to constitutionally guaranteed rights -- not to mention the fabric of democracy -- are evident.

A third example of post-September 11 behaviors regards the overt manipulation and falsification of the historical record by the White House. On May 1, 2003, the White House Press Office issued an official statement saying "President Bush Announces Combat Operations in Iraq Have Ended." As it became increasingly clear that the war was far from over, the president's public relations campaign ("mission accomplished") backfired, drawing comments from critics, and leading the president to equivocate. By 19 August, 2003, *The Cursor* discovered that the May release had been changed to reflect a more nuanced position, consistent with the president's equivocation: "President Bush Announces *Major* Combat Operations in Iraq Have Ended." Thanks to the Internet Archive, the changes to the Press Office record could be traced and exposed, an action that resulted in a White House legal challenge to the archiving of its public statements by anyone other than itself.[7]

These three examples point to an interlocking strategy of removing information from the public sphere, denying members of the public the right to challenge or even speak about certain governmental activities, and falsifying the public record – activities all carried out under the cover of protecting state security. And at least in the first two cases, where quantification is possible, these activities are talking place at historically unprecedented levels. In and of themselves, these practices raise serious questions about the ability of a democracy to function when the activities of its government are shielded from public view. If information and state actions are hidden from view and held to be beyond public interrogation, if the government re-writes its own history and then legally challenges those who expose such activities, the notion of a state formed "by, for and of the people" seems very much in jeopardy. The situation is even more distressing if we recall the great strides that have taken place in surveillance, both by the state and the private sector. Projects with global reach such as the National Security Administration's ESCHELON (a joint US/UK development), which according to a European Parliament report is capable of tracking and decrypting messaging sent via radio, satellite, microwave, cellular or fiber-optic means[8]; regulations requiring banks to report all transactions over $10,000; the credit card data regularly "mined" by market analysts; the routine scrutiny of all airline passenger data; and the network of 'smart' cameras that track cities and roadways, all have inherent potentials for abuse if not protected, and, as seems to be immanent, if interlinked. Indeed, issues of what is appropriately private and what should be open for government scrutiny should be central issues of public debate, but the current climate of secrecy has not encouraged such reflection.[9] And the situation is compounded by the steady growth in media concentration, where thanks to federal deregulation, seven media conglomerates (Disney, CBS, Time Warner, News Corp, Bertelsmann AG, Viacom and General Electric) currently control by some counts more than 90% of the American media market. While the fact that media outlets owe their market dominance to the government does not in itself argue for

conspiratorial behavior, neither does it argue for robust pluralism of opinion, independence of thought, or critical (and thus 'controversial') interrogation of governmental actions shrouded in state security and designed to prevent terrorism.[10] As an ensemble, these elements have the makings of a paranoid's nightmare.

securing the state: social media 2.0

But beyond media concentration and enhanced surveillance capacities, what of the third environmental change to the media landscape -- networked computing, peer-to-peer communication, *social media*? The contrast with levels of concentration in the traditional media sector couldn't be more dramatic; and while open to surveillance, transparency in general is one of the system's great strengths. Before making the case for social media, let's first situate its relevance in terms of the foregoing narrative. If one of the most proximate threats to state security is a regime of governmental secrecy, and through it both slippage in the identities of the government and state, and removal of the activities of government from public oversight, what can social media bring to the table? One answer was provided long ago by one of America's founding fathers. Thomas Jefferson summarized the principle of distributed access as a way to keep vital information available and the principles of state within universal reach. Speaking of ways to assure the preservation of America's founding documents, Jefferson said:

...let us save what remains: not by vaults and locks which fence them from the public eye and use in consigning them to the waste of time, but by such a multiplication of copies, as shall place them beyond the reach of accident.[11]

A clearer and more succinct summary of the differences between the policies of the current secrecy-obsessed US government and the possibilities afforded by networked computers is difficult to imagine. Although Jefferson was speaking of the documents outlining the foundations of the US state, including its constitution that has been under siege of late, his insight can be extended. Public access and the widespread multiplication of information offers the surest way to keep a society open, informed, critical, and free of the manipulation and 'accidents' that seem to plague post 9/11 American information flow.

Let's first step back and consider the nature of social media. In a world where people increasingly manage, direct and re-define when and where they experience media, how they share it, and what it means to produce and consume, we need to think about cultural processes in dramatically new ways. The shifts from analog to digital, from centralized to dispersed, from mass media to social media, from information transmission to collective intelligence, from old statistical extrapolations to new data feeds, all point to media use that is social by design, not social by default. The descriptors used by Tim O'Reilly and others for Web 2.0 are revealing: 'an architecture of participation,' 'harnessing collective intelligence,' 'exchanging,' 'pooling,' 'collaboration,' ....[12] Whether we look to social media communities such as *technorati*, or social networking sites such as *friendster* and *myspace*, or media fashion communities such as *digg*, we see new logics that have to be understood if we are to make use of them. Before looking a bit more closely at what these developments portend for the state and security, first a few words about the technologies that have been drawn upon. The World Wide Web was largely made possible thanks to the introduction of mosaic and the Pentium chip a little

over twelve years ago (ca 1995). Making far more effective use of networked computers, these developments were also aided by significant increases in cable carrying capacity (broadband), compression algorithms, and cheap memory. These developments have continued, and two parameters in particular have bearing on my argument: memory and transmission speed. Memory capacity is growing ever vaster and cheaper as a look at the retail electronics sector will demonstrate. As production capacities grow, so too does our ability to hold the massive amounts of data that are being produced. Transmission speeds have also improved significantly, with Japan's Kansai Electric demonstrating in 2005 a transmission rate of one tarabit per second, or the equivalent of a two-hour film in 0,5 seconds. Together, massive increases in memory and the new transmission speeds combine with a near geometrical progression of wired households in some national contexts to suggest that the developments we've seen since the introduction of mosaic just over a decade ago are but the tip of an iceberg.

The challenges posed to the old order by the collaborative logics of Web 2.0 can be seen in many sectors. Collaborative news networks such as Slashdot (www.slashdot.org) and Kuro5hin (www.kuro5hin.org) have blurred the distinctions among editors, readers and writers, with their participants fulfilling all roles. They draw on correspondents and commentaries from around the world, complicating, contradicting, and compositing various bits of information so that the reader must actively consider multiple points of view and sources before making a determination about the news, in the process enhancing citizenly engagement. In a similar way, open source software initiatives such as Linux draw upon a community of collaborators, and by keeping the source code open, they direct their energies towards improving functionality rather than building encryption systems and expending resources in litigation. Moreover, with ample networked input and development, they have the advantage that their software mutates and improves more quickly than proprietary models. Add low costs into the mix, and it is little wonder that Linux is steadily winning terrain from centralized companies such as Microsoft.[13] The contrast between the two governance structures – one open, community directed, and structured through common purpose, the other heavily encrypted, centralized and driven by profits – obviously holds lessons for the larger political scene.

Decentralized, networked, collaborative, accretive, ephemeral and dynamic… social media differ fundamentally from the media around which our institutional traditions have been constructed. Their rootedness in community and collaborative interactions, and their responsiveness to an ever-present XXX, gives them a unique quality as finely-grained embodiments of culture. Of all the differences from traditional media discussed above, perhaps the two most difficult ones are 1) the notion that these media are open, dynamic and always in progress rather than having a final, completed state; and 2) that these media are networked, and that the web of connections bears heavily on the meaning of any one site. These two parameters are not only unfamiliar, but somewhat daunting in terms of their potential storage requirements for records of state and the documentation of the governance process, where stability, integrity, and scale are thorny issues. Fortunately, as mentioned above, memory is getting cheaper by the day and transmission speeds are improving significantly. But just as importantly, the very distributed logic that enables social media and peer-to-peer applications holds solutions to these problems. Consider music file exchanges such as Napster or Grokster and the like. They managed something well beyond the physical (let alone financial) capacities of the traditional music industry by digitalizing a vast amount of music, storing it, and

distributing it on demand to millions of users. They did this by informally networking millions of personal computers in homes across the world, building in integrity checks and protocols, and distributing the tasks of digitalization, storage and access in such a way that the cost was negligible and the labor involved was freely given. Millions of modestly-sized memory chips and processors, when properly linked, emerge as a formidable and robust computing force far beyond the potentials of any one centralized system. This network, the basis after all of social media, could also potentially be put to use as a decentralized state repository, complete with the redundancies, checks, and quality controls currently evident in many existing applications. And the best part is that there are working examples of this principle that demonstrate its robustness.

LOCKSS ("Lots of Copies Keep Stuff Safe" <www.lockss.org>) offers a splendid working example. In their own words,

> LOCKSS is open source software that provides librarians with an easy and inexpensive way to collect, store, preserve, and provide access to their own, local copy of authorized content they purchase. Running on standard desktop hardware and requiring almost no technical administration, LOCKSS converts a personal computer into a digital preservation appliance, creating low-cost, persistent, accessible copies of e-journal content as it is published. Since pages in these appliances are never flushed, the local community's access to that content is safeguarded. Accuracy and completeness of LOCKSS appliances is assured through a robust and secure, peer-to-peer polling and reputation system.[14]

Just as LOCKSS is exemplary of a solution that makes use of distributed computing, other examples have tackled the problem of capturing the dynamic and extensive character of the web (and thus have the capacity to capture the dynamic complex of state activities). Nearly synonymously with the appearance of the World Wide Web, Brewster Kahle initiated his remarkable Internet archive known as the Wayback Machine <www.archive.org>. With over 85 billion web pages archived since its inception in 1996, the archive is composed of “snapshots” of websites taken at regular intervals, allowing the interested researcher to go back in time and track changes. The previously mentioned ‘discrepancy’ in the White House Press Office’s re-writing of a press release, or attempts to re-write the cv’s of Enron officials after their company’s collapse, or the forgery of President Bush’s military records all came to light thanks to on-line archives. For the engaged citizen, the ability to track the emergence of the public record, documents of state, regulatory processes, the ‘public’ function of the court system, etc., is an invaluable resource. And the best part is that Mr. Kahle managed to capture the dynamic character of the web with a modest infrastructure and limited budget. With a mirror site in Alexandria, Egypt, the archive’s discursive claim is loud, clear and, I think, not at all overstated. With a more fulsome budget, the archive could expand its operations and the frequency of its ‘snapshots’, but for the moment, its beauty is that it works efficiently and outside the entanglements of national governments and funding agencies. For once in our media history, someone has managed to both think ahead and act accordingly.

LOCKSS and the Wayback Machine, both essentially accessible and distributed archiving systems, offer two splendid examples of what is possible, one growing out of the efforts of progressive librarians and the other from an insightful and resourceful individual. Are these a model for the open state, seeking to hew to the spirit of Thomas Jefferson’s notion of multiplicity, access and openness? They certainly offer a dramatic

alternative to the cult of secrecy that has infected post 9/11 American governance. Are there challenges? Of course. But there are clear solutions as well. Distributed knowledge like distributed power is fundamental to the workings of a democracy, and both of these systems demonstrate the feasibility of this Jeffersonian ideal by relying on new technologies. Data stability and freedom from intentional or unintentional information corruption are *sina qua nons* of state documents, and again the robustness of LOCKSS and the Wayback Machine demonstrates levels of security that appear to exceed those of the Pentagon's computers. Scalability is a fundamental issue, particularly for the affairs of state where volume and dynamism both pose great demands. The Wayback Machine's 85 billion plus pages shows not only that capacity is not an issue, but more importantly that navigating one's way within such a vast data repository is not problematic. Moreover, the emergence of the semantic web and the move towards Web 3.0 promise even more effective search logics.

Just as important as these demonstrated technological capacities are the attendant and profound shifts that have been taking place in some of our cultural practices. The controversy surrounding music file exchanges such as Napster and Grockster accelerated transformations in the music industry, but did something more: they helped to redefine 'music' from a commodity bought at a store, to a social relationship exchanged between friends or fans. Collaborative news networks such as Slashdot redefined 'news' from an authorized point of view (or 'truth') to an active process of comparison, criticism, and evaluation. And open source software helped to transform 'software' from a heavily marketed and encrypted commodity to something more like language – open, community based, and responsive. These changes and many like them have caught the imagination of a new generation, and while the established music, news media, and software industries are doing their best to put the genie back into the bottle, the overall center of gravity continues to shift in the direction of an engaged and participatory culture. From this perspective, the culture of the state, too, is subject to change. Like other panicked industries, it can entrench itself in old privileges and fight a defensive war by focusing on secrecy and centralized power; or it can take advantage of the new affordances, embracing opportunities to enhance communities of participation, openness, and citizenly engagement.

Conclusion

The changes that characterize the shift to Web 2.0, from the center to the distributed, from social by default to social by design, are manifesting themselves in international financial markets, in mainstream industries such as IBM, in global flows of peoples and labor processes. The change will not be easy, certainly for those with vested interests in long-standing institutional processes. But it is also increasingly evident that like it or not, change is coming, and with it opportunities to evaluate our principles, and to reengage our imagination. The open and robust systems described above are examples of ways the government could handle many of the affairs of state, making the governance process transparent, making the records of state open and available, and encouraging a climate of participation. The redundancy and distributed nature of these configurations renders them immune from terrorist or enemy attack (unlike highly centralized information repositories) – the reason, after all, for the development of ARPANET, the US Defense Department's initial version of the Internet. And transparency and access to the process of governance is the best defense to the

sorts of internal dangers to the integrity of the state that we have witnessed in the US since the events of September 11. Issues of privacy and surveillance, like those of intellectual property in the commercial sector, remain problems. But at least in the surveillance sector, issues of power only emerge when there is an imbalance, when one group 'sees' and the other is 'observed.' Although an equal playing field is not the answer, it at least keeps things sporting until such time as we have resolved the larger ethical quandary.

From Thomas Jefferson to Thomas Kean, we have had a steady if small stream of leaders who have noted the dangers of secrecy to the security of the state, and the benefits of openness to the state's health. Terror, though reprehensible, ultimately affects lives and property; but the security of the state is only threatened when its principles and historically accrued and refined values are subverted. Terror can certainly be used to bring about that subversion, but this requires active collusion within the government. Mobilizing through fear and masking through secrecy, all in the name of security ... or responding through informed and critical collaboration? The security of the state hangs in the balance.

[1] Although the transient political dimension of government is a key issue here, it is not my goal to blame the Republican Party, which at the time of these events, held the presidency and majorities in both houses of congress. Instead, a highly motivated cohort within the political leadership was able to use the power of the state to frighten and bully a majority of both parties into doing its bidding.

[2] In this regard, the early 2007 legal actions taken by Spain, Italy and Germany against members of America's CIA charged with kidnapping and illegally imprisoning their citizens deserve credit, as do their investigations into their governments' complicity in 'extraordinary renditions' by permitting the US to use their airports and airspace to transport untried suspects to third countries for torture.

[3] *Oxford English Dictionary*, Second Edition (1989)

[4] The Bush administration's imprisonment of terror suspects without a trial of their peers circumvents a legal tradition grounded in Paragraphs 38 and 39 of the *Magna Carta*. *38: In future no official shall place a man on trial upon his own unsupported statement, without producing credible witnesses to the truth of it. 39: No free man shall be seized or imprisoned, or stripped of his rights or possessions, or outlawed or exiled, or deprived of his standing in any other way, nor will we proceed with force against him, or send others to do so, except by the lawful judgment of his equals or by the law of the land.* When, in1627, King Charles I invoked his right to simply imprison anybody he wanted, he declared (not so differently from the Bush administration) "per speciale Mandatum Domini Regis." Parliament responded with the1628 "Petition of Right" law, later strengthened with the "Habeas Corpus Act of 1640" and a second "Habeas Corpus Act of 1679," all reiterated in the 4th through 8th amendments to the US constitution.

[5] Scott Shane, "Increase in the Number of Documents Classified by the Government" *The New York Times*, July 3, 2005.

[6] Rebecca Carr, "State Secret Privilege Use Increases Under Bush," *Cox News Service* June 21, 2006.

[7] http://www.thememoryhole.org/pol/iraq-combat/ See also http://www.cursor.org

[8] http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf (May 18, 2001)

[9] The state's role in safeguarding privacy can also be seen as part of the security it provides to its citizens, a topic that I will not take up in this chapter. For reflections on the topic in a Dutch context, see Geert Munnichs, "Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21e eeuw" (Rathenau Instituut/Universiteit Tilburg, February 2007).

[10] Consider the American press's almost universal acceptance of the government's ban on showing coffins of dead American soldiers, let alone the dead outside of coffins; or compare visual coverage of the Iraq or Afghanistan wars' effects on their populations between the US media and even the British press.

[11] Jefferson, Thomas. [1791] 1984. Thomas Jefferson to Ebenezer Hazard, Philadelphia, February 18, 1791. In Thomas Jefferson: *Writings: Autobiography, Notes on the State of Virginia, Public and Private Papers, Addresses, Letters*, edited by Merrill D. Peterson. New York: Library of America. Cited on the homepage of LOCKSS.

[12] Tim O'Reilly, "What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software" (9/30/2005)
http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

[13] The implications to these and related changes to culture, society and the economy are profound, and have been discussed by a number of recent studies. Among the most prominent are Yochai Benkler, The Wealth of Networks (Yale University Press, 2006) and Henry Jenkins, *Convergence Culture* (New York University Press, 2006).

[14] http://www.lockss.org/lockss/About_LOCKSS