
Douglas Thomas
Annenberg School for Communication
University of Southern California

As you begin playing the latest MP3 file downloaded from the Internet your computer flashes an ominous warning. A few second later your computer shuts down and you are unable to turn it back on. The work of malicious hackers? The result of the latest virus? The work of cyber-terrorists disrupting the Internet? The answer becomes apparent a few days later when you receive a summons to appear in court for federal copyright infringement. Before it stopped working, your now defunct computer forwarded a list of suspicious files to the record companies. Legislation currently under consideration by Congress would make such scenario not only likely, but also perfectly legal. At the same time, computer chip manufactures, software producers and record company executives are hard at work, bringing products to market to make it a reality.

While many of our worst fears about the future of the Internet circulate around notions of hackers, viruses and cyber-terrorists, the real threat to our individual freedoms and liberties are grounded in a threat much closer to home—Digital Rights Management, information security, and domestic surveillance. As the number of cameras, recording devices, and monitoring apparatuses grows larger each year, the public is offered cataclysmic scenarios of financial ruin and devastating loss of life as the result of a few mouse clicks or carefully written code by cyber-terrorists.¹ In reality such threats are nearly non-existent.² Why then are stories of cyber-terrorists using the Internet to attack American power plants, airlines, hospitals and food services so widespread?

The answer has more to do with record companies, Walt Disney, and corporate databases than we might possibly imagine. While the myth of cyber-terror and malicious hack attacks circulate everywhere, the reality is far more insidious and poses a threat unlike any we have previously encountered. As we become accustomed to increasing levels of domestic surveillance in the workplace, in public spaces, and even in our homes, corporate interests are beginning to align with law enforcement to offer previously


unthinkable devices to monitor every aspect of daily life, a kind of Pascal’s wager, where every option is weighed in contrast to the ever-present threat of international terrorism.

In the wake of September 11th, there has been a renewed interest in cybersecurity. Terrorists, it is feared, are likely to attack on all fronts and one of our greatest vulnerabilities may be our reliance on the Internet for commerce, communication, and even the basic necessities of everyday life.

A terrorist attack that would result in significant loss of life or catastrophic economic impact is not only unlikely; by most accounts it is impossible. Why then do we have such a fascination with the idea of cyberterrorism? The answer rests, at least in part, with the very idea of technology itself and ways in which we have become increasingly reliant on machines and devices with little understanding of their inner workings or design. Even as technology appears mysterious and opaque to the majority, we harbor a sneaking suspicion that those who understand the way in which technology works are able wreak havoc with a few simple keystrokes. With the right knowledge, people fear that terrorists could crash planes, cripple the stock exchange, shut down the power grid, and even poison children’s breakfast cereal. The reality of the situation is that such attacks are virtually impossible to accomplish, have a low probability for success and are easy to prevent with a few simple counter-measures. Terrorist are much more likely to use bombs, bullets or more traditional weapons to attack a country’s infrastructure.

In short, the lesson of September 11th is that not all 21st century warfare will be information war. The weapons of terror are not modems and CPUs, they are box cutters and shoe bombs. What then is the investment in fighting the war on terror as an information war?

Because America has enjoyed an extended period of technological growth and innovation, we have grown accustomed to finding technological solutions to complex social and political problems. Recent wars in Kosovo and the Persian Gulf have been fought and sold as “hi tech” wars with few American casualties, precision “surgical” strikes and limited collateral damage. They have been wars of “control” where superior technology has provided a sense of comfort, distance, and safety.

September 11th refocused the issue of control back upon the domestic landscape. While US intelligence agencies are able to engage in surveillance with impunity in foreign countries, domestic surveillance has always been highly regulated, monitored and limited. In fact, our best intelligence agencies are not chartered for domestic surveillance. To respond to problem of domestic surveillance, DARPA initiated work on a new program to reassert control and fight the war on terror on the home front.

Proposed by DARPA in the Fall of 2002, Total Information Awareness is an effort “to revolutionize the ability of the United States to detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts.” The manner in which TIA intends to do this is by consolidating federal, state and local government and corporate databases to
find connections between “transactions” such as passports; visas; work permits; driver's license; credit card; airline tickets; rental cars; gun purchases; chemical purchases and “events” such as arrest or suspicious activities.

Total Information Awareness is a first step in treating the war on terror as an “information war,” presuming that sorting database information to connect “transactions” and “events” is likely to “detect, classify and identify foreign terrorists.” While the justification for Total Information Awareness is explicitly aimed at terrorism, the actual uses of the system will be left up to national, state and local law enforcement agencies.

Coupled with the Patriot act and other efforts at Homeland Security, recent legislation has made domestic surveillance a top priority for law enforcement and has extended unprecedented privileges to governments and law enforcement to obtain information. Privileging “information” in the war on terror is aimed more toward a growing agenda for implementing an infrastructure for domestic surveillance then it is at identifying foreign terrorists or terrorist threats.

As the government ramps up its surveillance program, industry is not far behind. Domestic surveillance is a cornerstone of recent efforts to ensure copyright protection for major record labels and the movie industry. Amidst fears of declining sales, piracy and peer to peer file sharing, both the RIAA and MMPA have lobbied for stringer copyright protection for their industry products.

The industry had its first victory with the Digital Millennium Copyright Act and has had subsequent successes in the extension of copyright and the suppression of computer code designed to give access to encrypted DVDs.

As issues of Digital Rights Management (DRM) take center stage, major hardware and software manufacturers are beginning their own offensive, offering a new platform of “Trusted Computing” which will integrate surveillance and content management into new hardware and software, among them Intel’s processing chips as well as Windows operating system software.

As Richard Clarke, Special Advisor to the President for Cyber Security, explained in a dinner address at Microsoft’s Trusted Computing Forum in 2001, “There is a parallel between terrorism and information security . . . . We need to create islands -- islands in the Internet, if you will -- where when you land on those islands you have to show some identification.”

In what follows I want to trace out the implications of the transformation from a system of human-based security to a system of physical security, analyzing the impacts on questions of copyright and intellectual property, information security, and domestic surveillance.
Get the People Out of the Loop

To anyone familiar with the history of popular representations of technological dystopias, the idea of removing the “human element,” seems strikingly familiar. One of our deepest cultural fears is based in the premise that when humans cede authority and decision making to machines, disaster soon follows. Figures such as HAL from 2001, the terminator, or WOPR from WarGames all give embodiment to our deepest suspicions.

Those fictions give voice to many of our expectant anxieties about technology, with the most basic being the acceptance of the trade off between notions of freedom and security. The premise is simple; the more secure a system is, the less freedom and choice an end user has. One of the most basic ways to secure a system then is by decreasing a user’s agency. In doing so, the system is able to do less, but it is able to do those things with a greater degree of security.

Perhaps the most well known vulnerability in any secure system is the people who use it. That basic vulnerability is the result of this basic trade off between security and use. The more secure a system is, the more difficult it is to use. The easier it is to use, generally, the less secure the system will be. The modern paradigm of security has three central components: a secret, a code, and a body. Of those three elements, the last seems fundamentally out of place. Accordingly, it is the one which the latest effort of Trusted Computing seeks to replace. We can see how the “problem of the body” plays out at the most basic level of security by looking at encryption, which is at the heart of the proposed model of Trusted Computing.

Encryption, as the process of encoding and enciphering text, appears on its surface as act of pure code. On the surface, it appears to have nothing to do with the body. Recent algorithms have reduced encryption almost entirely to the language of mathematics. Public key encryption, the standard for most Internet and government work, relies on mathematics no more complicated than basic prime number theory, algebra and modulus arithmetic. The principle of modern encryption is simple: one finds a mathematical problem that is simple to pose and impossible to solve without a key. Modern encryption utilizes even more sophisticated “one way” functions, allowing a code to have two different keys, one that locks and one that unlocks, neither of which can be derived from the other. The triumph of modern encryption is the removal of the body, rendering encryption an act of pure code. Early efforts at encryption required a secret to be shared, passed from one body to another. It was predicated on both parties knowing the same secret, but our latest efforts remove even that problem. No one needs to know your code, your secret or your password, not even the computer.

The history of encryption, however, tells a different story. In telling it, we begin not with mathematics or computers, nor with the codebreakers of the Second World War, or even as some have suggested with Julius Caesar scrambling messages to troop commanders in Rome. The history of encryption begins with the last book of Oedipus trilogy, Oedipus at

---

Colonus, where three discrete elements merge in the first narrative of encryption. Oedipus, fearing his grave would be defiled, before dying extracts a promise from the King of Athens, that he keeps the place of his burial (literally his crypt) secret. In exchange, Oedipus offers Athens perpetual safety from its enemies as long as the secret is maintained. These three components comprise the base elements of the technology of encryption: a code, the body and the protection of the state.

It also marks the body as the disruptive element which continually threatens not only the normative structure of code, but the very security of the state itself, especially when that body, like Oedipus’s is a transgressive one, marked by its violation of code and its transgression of the law.

**Trusted Computing**

The latest, and most significant attempt to excise the body from the system is “Trusted Computing,” the brand name for a new industry collective, which includes chip manufactures Intel and AMD, Microsoft, HP, IBM, Sony and Sun Microsystems. Their stated goal is as follows: “The Trusted Computing Group is enabling open and widely available building blocks and common interface stacks that the industry can adopt across multiple platform types and environments. With these open building blocks, the industry can address a range of security needs without compromising functional integrity, privacy or individual rights.” Throughout their website, The Trusted Computing Group (TCG), deploys language of openness, transparency and even the language of civil liberties to describe their project. Although one might reasonably treat these claims with suspicion, my effort in this essay is neither to challenge nor undermine the motives of the industry, but, instead, it is to trace of the implications of what it means to shift issues of security away from the user and toward the machinery itself, in some cases all the way down to the CPU.

As Trusted Computing has evolved, so has the discourse. What was initially described as an insistence that there be no compromising of individual rights and privacy, as of July 13th, 2005 had morphed into a new phrase: “TCG specifications are designed to enable more secure computing environments without compromising functional integrity with the primary goal of helping users to protect their information assets from compromise due to external software attack and physical theft.” Concerns about privacy and rights have now been trumped by issues of attack and theft, again deploying the traditional trade off between security and freedom.

The difference between the two statements may be subtle, but the distinction is important. What is at stake is the question of user agency. Privacy and individual rights mean

---

4 Sophocles, Oedipus at Colonus, see especially lines 1732-1740.
something very specific in the context of the software community. As Richard Stallman, perhaps the most vocal opponent of the Trusted Computing platform sees it: “Who should your computer take its orders from? Most people think their computers should obey them, not obey someone else. With a plan they call "trusted computing", large media corporations (including the movie companies and record companies), together with computer companies such as Microsoft and Intel, are planning to make your computer obey them instead of you. (Microsoft's version of this scheme is called "Palladium".) Proprietary programs have included malicious features before, but this plan would make it universal.”

The discourse that has spawned around Trusted Computing puts user agency at the center of the debate over what constitutes “trust” as well as what the rights of individual users are in relation to their hardware and software. Even the name itself, “Trusted Computing” speaks to the question of agency and the end user. The formulation of the notion of trust into a past participle already implies a lack of agency on the part of the end user. Acceptance of the name provides assent to a relationship which is already governed by the hardware itself. That is to say, ownership and usage presuppose trust.

In what follows I want to sketch out a political economy of trust around three issues: time, content, and degree. Or put into a series of questions.

1. When do we trust?
2. Who do we trust?
3. How much do we trust them?

In each case, I want to use a basic example to examine the interconnections among trust, agency, and the body to try to understand the broad implications of the shift to a new way of thinking about trusted computing. Those three examples are copyright and IP, information security, and domestic surveillance.

**Copyright and IP (When Do We Trust?)**

It has become a commonplace today to pit notions of innovation against restrictive regimes of copyright and intellectual property rights. Larry Lessig’s contention that law has been used to increase corporate protection at the expense of the commons has emerged as a central topos is the debate over intellectual property. But even Lessig’s solution, the institution of a “creative commons,” merely repeats the problems of the old system, albeit in a less restrictive and more content-producer friendly way. It is at this level that I want to take issue with Lessig’s conflation of the terms code and law.

---

The fundamental conflict is not an intellectual one. That is to say, most people have concerned themselves with drawing the boundaries around what is protected, in an effort to determine the proper scope and boundaries of intellectual property and copyright. The fundamental conflict, instead, is a temporal one. What is important in the discussion is not so much what boundaries are drawn as it is when they are drawn.

Whether you take a restrictive test, such as the DMCA or a more open framework such as Lessig’s Creative Common’s license, the true utility of these frameworks rests not in their construction, but in their application.

The primary issue with Trusted Computing, then, is that it takes intellectual property and DRM as an engineering question, rather than as a legal question. As any good engineer will tell you, engineering considers most problems from the perspective of design and in terms of what Science and Technology Studies people refer to as affordances. Technologies, therefore, make certain things possible and remove other possibilities; they provide and limit affordances, according to particular needs or functions.

Most technologies today provide affordances for both legal and illegal use of content. Which is to say, the decision about what is and is not “legal” is relegated to the legal system. Infringement is decided as a matter of application of law and it determined after the point of action. The great advantage of such determination is that it allows for flexibility of interpretation, change, and evolution.

The issue with Trusted Computing, then, in terms of IP, is that it treats copyright and intellectual property protection as a design issue. It eliminates the possibility of use, before that use can be determined to be fair or not. In short, it treats what is rightfully a legal question as a design question and in doing so eliminates the possibility of application, change or evolution.

The goal of Trusted Computing is the removal of the interpretive body, the system of application, which is to say judgment from the system of evaluation.

**Information Security (Who Do We Trust?)**

The problems of Trusted Computing for security mirror the issues addressed with IP. But in the case of security, matters of agency figure in at a different level. The question of agency within this framework is really a matter of how you think about security. Is security a centralized or distributed problem? If it is the first kind of problem, which people like Richard Clark seem to believe it is, then Trusted Computing makes a lot of sense. In short if security is a matter of whether or not our walls are good enough, strong enough or high enough, then centralizing the problem and inventing better walls is an appropriate solution.

People like Bruce Schneier, however, argue that such a metaphor is incomplete, “Because the Net is so often compared to a fortress,” he writes, “most Internet security relies on prevention. That's not bad, but it's incomplete. Prevention is the least effective solution,
because it's static and passive.” In contrast, people like Schneier and others see security as a dynamic and often times decentralized problem.

For every secure product released, there are thousands of hackers, security analysts, cryptographers and “script kiddies” doing their best to break in, hack, circumvent and penetrate the code. They exist both in isolation and in communities. Some report findings to the compromised companies, others never do. Some release information publicly, others write patches and workarounds to secure software and platforms from attack. Often times, however, the best security fixes and products come not from the producers of the hardware and software, but instead from security communities and even more often from third party companies that emerge to sell security as an “add on” service (e.g. Norton, F-Secure, Symantec, ZoneAlarm, SpyBot, Ad-Aware and so on).

The way in which the end user trusts, then, relies in large part on the ability of third parties to both hack and protect the systems from invasion. The issue of trust, then, like the issue of security can been seen as a centralized or decentralized one, one which pits security, in the case of the Trusted Computing Platform, versus freedom, in the case of the decentralized selection of products or devices which allow a user to customize his or her level and degree of security.

**Domestic Surveillance (How Much Do We Trust Them?)**

Of course there is no small irony in the idea that while the body has been excised from two of the most crucial and important aspects of technological innovation, it reappears front and center in the third, as an issue of domestic surveillance.

The three principle players that are involved in the discussion of Trusted Computing are the hardware and software industry (think Intel, AMD, IBM, Microsoft), the entertainment industry (think Sony, Disney, BMG) and the government. These three interests have had primarily antagonistic relationships with one another. The computer industry has been at odds with government over anti-trust issues, the entertainment industry has been at odds with the government over censorship issues and regulation and with the technology industry around issues of piracy.

Around issues of Trusted Computing, however, for the first time all three of these interests align around issues of domestic surveillance. In short, the technology industry, the entertainment industry and the government all have a vested interest in knowing what is happening inside each and every computer on every desktop.

The protection of the public has rested on two central ideas. First, that the hardware and software infrastructure was sufficiently open to allow independent experts to audit how the technology was being used and second, that the antagonisms between and among the three parties provided enough flow of influence and money among decision makers to ensure that nothing particularly drastic would find its way into law or into the hardware.

---

and software. The Digital Millennium Copyright Act signaled a shift in the second way of thinking and Trusted Computing signals a shift in the first.

The combination of these two, however, creates a truly problematic scenario. The premise of Trusted Computing is to secure the system at the most basic, even physical, layer. In doing so, it is able ensure that security provisions are not being bypassed or circumvented. In other words, it no longer limits access to what the user can do, it limits what the technology itself is able to do. It literally evokes the past participle, trusted, by guaranteeing that the hardware itself can already be trusted. In fact, one could go as far as to argue that the embedding of security in the hardware itself could eliminate suspicion from the computer itself. Trusted Computing then, cannot not be trusted.

But what exactly are we trusting and how can we know the degree to which that trust is granted? The answer is that we can’t. Provisions in the DMCA and the EU Copyright Directive make it illegal to understand not only how Trusted Computing works, but also what it is doing.

Ironically, in order to be trusted, by its very definition, your computer must have access to and knowledge of what the user is doing. As Bruce Schneier reminds us, that definition the definition of trust itself is about eliminating agency, not necessarily about increasing peace of mind: “A "trusted" computer does not mean a computer that is trustworthy. The DoD's definition of a trusted system is one that can break your security policy; i.e., a system that you are forced to trust because you have no choice.”

---