

We Lost the War. Welcome to the World of Tomorrow

FRANK RIEGER

Losing a war is never a pretty situation. So it is no wonder that most people do not like to acknowledge that we have lost. We had a reasonable chance to tame the wild beast of universal surveillance technology, approximately until 10 September 2001. One day later, we had lost. All the hopes we had, of keeping the big corporations and security forces at bay, and of developing interesting alternative concepts in the virtual world, evaporated with the smoke clouds of the collapsing World Trade Center.

Just right before that, everything looked not too bad. We had survived Y2K with barely a scratch. The world's outlook remained mildly optimistic despite all the millennial projections. The New Economy bubble gave most of us fun things to do, and the fleeting hope of plenty of cash not so far down the road. We had won the Clipper-chip battle,¹ and crypto-regulation as we knew it was a thing of the past. The waves of technology development seemed to work in favour of freedom, most of the time. The future looked like a yellow brick road to a nirvana of endless bandwidth, the rule of ideas over matter, and dissolving nation states. The big corporations were at our mercy because we knew what the future would look like, and we had the technology to build it.

Those were the days. Remember them for your grandchildren's bedtime stories. They will never come back again.

We are now deep inside the other kind of future, the future that we speculated about as a worst-case scenario, back then. This is the ugly future, the one we never wanted, the one that we fought to prevent. We failed. Probably it was not even our fault. But we are forced to live in it now.

Democracy is already over.

By their very nature, the Western democracies have become a playground for lobbyists, industry interests and conspiracies that have absolutely no interest in real democracy. The democracy show must go on, nonetheless. Conveniently, the show consumes the energy of those that might otherwise become dangerous to the status quo. The show provides the necessary excuses when things go wrong, and keeps up the illusion of participation. Also, the system provides organised and regulated battleground rules to find out which interest groups and conspiracies have the upper hand for a while. Most of the time it prevents open and violent power struggles that could destabilise everything. So it is in the best interest of most players to keep at least certain elements of the current democracy show alive. Even for the more evil conspiracies present around us, the system is useful as it is. Certainly, the features that could provide unpleasant surprises, such as direct popular votes on key issues, are the least likely to survive in the long run.

Of course, those in power want to minimise the influence of random chaotic outbursts of popular will as much as possible. The real decisions in government are not made by ministers or the parliament. The real power of government rests with the undersecretaries and other senior non-elected civil servants, who stay while the politicians come and go. Especially in the bureaucracies of the intelligence agencies, the ministry of the interior, the military, and other key nodes of power, long-term planning and decision-making is not left to incompetent mediocre political actors who are elected more or less at random. Long-term stability is a highly valued thing in power relations. So even if the politicians of states suddenly start to be hostile to each other, their intelligence agencies will often continue to cooperate and trade telecommunication interception results as if nothing has happened.

Let's try for a minute to look at the world from the perspective of one such 60-year-old bureaucrat who has access to the key data, the privilege of being paid to think ahead, and the task of preparing policy for the next decades. This is what he might foresee:

First: The place of paid manual labour will be eroded further by technology, even more rapidly than today. Robotics will evolve far enough to kill a sizeable chunk of the remaining low-end manual jobs. Of course, there will be new jobs; servicing the robots, biotech, improving design, experimenting with nanotechnology, etc. But these will be few, as compared with the number of jobs today, and require higher education. Globalisation continues its merciless course and will also dictate the export of a lot of jobs of the brain-labour type to India and China, as soon as education levels there permit it.

So, Western societies will end up with a large percentage of its population, at least one-third, or possibly half, the number of employable people having no real paid work. There are those whose talents can be cheaply bought elsewhere, those who are more inclined to manual labour. This would include not only the undereducated, but also all those who simply cannot find a decent job anymore. This part of the population needs to be pacified, either by Disney or by Dictatorship, most probably by both. The dimensions of the unemployment problem severely affect the ability of states to pay for social benefits. At some point it becomes cheaper to put money into repressive police forces, and to rule by fear rather than put the money into payouts to the unemployed population and buy the necessary social

peace. Opportunities for criminal activity become more attractive when there is no decent job to be had. Violence is the unavoidable consequence of the further degradation of already unequal social standards. Universal surveillance might dampen the consequences for those who remain with some wealth to defend.

Second: Climate change increases the frequency and devastation of natural disasters, creating large-scale emergency situations. Depending on geography, large parts of land may become uninhabitable due to drought, flood, fires or plagues. This creates a multitude of unpleasant effects. A large number of people need to move; crop and livestock production shrink; industrial centres and cities may be damaged to the point where abandoning them is the only sensible choice left. The loss of property such as non-usable (or non-insurable) real estate will become a frightening truth. The resulting internal migratory pressures towards safe areas will become a significant problem. Properly trained personnel, equipment and supplies needed as a response to environmental emergencies will have to remain on standby all the time, eating up scarce government resources. The conscripted segments of national armed forces may be formed into disaster relief units, as they hang around anyway with no real job to do except securing fossil energy sources abroad and helping out the border police.

Third: Immigration pressure from neighbouring regions will rise in all Western countries. It looks as if the climate-related disaster will initially hit areas such as Africa and Latin America the hardest. The economy there is unlikely to cope any better than the Western countries, with globalisation and other problems ahead. So the number of people who want to migrate at all costs from there to somewhere inhabitable will rise substantially. The Western countries need a certain amount of immigration to fill up their demographic holes, but the number of people who want to come will be far higher than this. Managing a controlled immigration process according to demographic needs is a nasty task, one where things can only go wrong most of the time. The inevitable reaction will be a Fortress Europe: serious border controls and fortifications, frequent and omnipresent internal identity checks, fast and merciless deportation of illegal immigrants, biometrics on every possible corner. Technology for border control can be made quite efficient once ethical hurdles have fallen.

Fourth: At some point in the next decade, the energy crisis will strike with full force. Oil will cost a fortune, as it will no longer be possible to extend production capacities economically in order to meet the rising demand. Natural gas and coal will last a bit longer, a nuclear renaissance may dampen the worst of the pains. But the core fact remains: a massive change in energy infrastructure is unavoidable. Whether the transition will be harsh, painful and society-wrecking, or just annoying and expensive, depends on how soon the investments in new energy systems start on a massive scale as oil becomes too expensive to burn. Procrastination is a sure recipe for disaster. The geo-strategic and military race for the remaining large reserves of oil has already begun, and will cost a vast amount of money.

Fifth: We are on the verge of technological developments that may require draconian restrictions and controls to prevent the total disruption of society. Genetic engineering and other biotechnology as well as nanotechnology (and potentially free energy technologies if

they exist) will put immense powers into the hands of skilled and knowledgeable individuals. Given the general rise in paranoia, most people (and for sure those in power) will not continue to trust that common sense will prevent the worst. There will be a tendency to create controls that keep this kind of technology in the hands of trustworthy corporations or state entities. These controls, of course, need to be enforced; surveillance of the usual suspects must be put in place to ensure knowledge of potential dangers in advance. Science may no longer be a harmless, self-regulating domain but something that needs to be tightly controlled and regulated, at least in the critical areas. The measures needed to contain a potential global pandemic from the Strange Virus of the Year are just a subset of those needed to contain a nanotech or biotech disaster.

Now, what follows from this view of the world? What changes to society are required to cope with these trends, from the viewpoint of our 60-year-old power-broking bureaucrat?

Strategically, it all points to massive investments in the domain of internal security.

Presenting the problem to the population as a mutually exclusive choice ; between an uncertain dangerous freedom and an assured survival under the securing umbrella of the trustworthy state ; becomes easier the further the various crises develop. The more wealthy parts of the population will certainly require protection from illegal immigrants, criminals, terrorists; and implicitly also from the anger of less affluent citizens. And since the current system values rich people more than poor ones, the rich must get their protection. The security industry will certainly be of happy, eager assistance, especially where the state can no longer provide enough protection to suit the more privileged.

Traditional democratic values have been eroded to the point where most people don't care anymore. So the loss of the basic rights that our ancestors fought for not so long ago is at first happily accepted by a majority that can easily be scared into submission. Terrorism is the theme of the day; others will follow. And these themes can and will be used to mould Western societies into something that has never been seen before: a democratically legitimised police state, ruled by an elite free from accountability; a state committed to modes of total surveillance, made efficient and largely unobtrusive by modern technology. With the enemy (immigrants, terrorists, catastrophe victims, refugees, criminals, the poor, mad scientists, strange diseases) at the gates, the price that needs to be paid for security will seem acceptable.

Cooking up the terrorist threat by apparently stupid foreign policy and senseless intelligence operations provides a convenient method to initiate the establishment of a democratically legitimised police state. No one cares that car accidents alone kill many more people than terrorists do. The fear of terrorism accelerates social changes and catalyses the efforts to build the structures and tools required to suppress the coming waves of trouble.

What we today call anti-terrorism measures is the long-term, consciously planned preparation of those in power for the kind of world described above.

The Technologies of Oppression

We can imagine most of the surveillance and oppression technology rather well. Blanket CCTV coverage is reality in some cities already. Communication pattern analysis (who talks to whom at what times) is frighteningly effective. Movement pattern recording from cell phones, traffic monitoring systems and GPS tracking is the next wave that is just beginning. Shopping records (online, credit and rebate cards) are another source of juicy data. The integration of all these data sources into automated behaviour pattern analysis currently happens mostly on the dark side.

The key question with regard to establishing an effective surveillance-based police state is to keep it low-profile enough to let the ordinary citizen feel protected rather than threatened, at least until all the pieces are in place to make it permanent. The first principle of the 21st-century police state: All those who have nothing to hide should not be bothered unnecessarily. This goal becomes even more complicated, since with the increased availability of information on even minor everyday infringements, the moral pressure to prosecute will also rise. Intelligence agencies have always understood that effective work with interception results requires a thorough selection between cases where it is necessary to do something, and those (the majority) where it is best to just be silent and relish the covert pleasures of voyeurism.

Police forces in general (with a few exceptions), on the other hand, have the duty to act upon every crime or minor infringement they get knowledge of. Of course, they have a certain amount of discretion already. With access to all the kinds of data listed above, we will end up with a system of selective enforcement.

It is impossible to live in a complex society without violating a rule here and there from time to time, often even without noticing it. If all these violations are documented and available for prosecution, the whole fabric of society changes dramatically. The old sign for totalitarian societies ; arbitrary prosecution of political enemies ; becomes a reality within the framework of democratic rule-of-law states. As long as the people affected can be made to look like the enemy -theme of the day, the system can be used to silence opposition effectively. And at some point the switch to open automated prosecution and policing can be made, as any resistance to the system is by definition terrorism . Social development is paralysed; the rules of the law-and-order paradise can no longer be violated.

Now, emerging from the claustrophobic reality tunnel of said 60-year-old bureaucrat, we have to ask ourselves: where is hope for freedom, creativity and fun? To be honest, we need to assume that it will take a couple of decades before the pendulum will swing back in the direction of freedom, barring a total breakdown of civilisation as we know it.

Only when the oppression becomes so directly overwhelming will there be a chance to reclaim the more progressive ideologies of earlier times, as people will have no choice but to resist and revolt. But as long as the powers-that-be continue to manage the system smoothly and skillfully, we cannot make any prediction as to when the new dark ages will be over.

So what now?

Move to the mountains, become a gardener or carpenter, search for happiness in communities of likeminded people, in isolation from the rest of the world?

The idea has lost its charm for most who ever honestly tried. It may work if you can find eternal happiness in milking cows at five o'clock in the morning. But for the rest of us, the only realistic option is to try to live in, with, and from the world, regardless of how oppressive it has become. And we need to continue to build our own communities, be they virtual or real.

The Politics and Lobbying Game

So where to put your energy, then? Trying to play the political game, fighting against software patents, surveillance laws, and privacy invasions in parliament and the courts can be the job of a lifetime. The advantage is that you will win a battle from time to time, and can probably slow things down. You may even be able to prevent a gross atrocity here and there. But in the end, the development of technology and the panic level of the general population will chew a lot of your victories for breakfast.

This is not to discount the work and dedication of those of us who fight on this front. But you need to have a lawyer's mindset and a very high tolerance of frustration to gain satisfaction from your efforts, and everyone does not have this quality. We will always need the lawyers.

Talent and Ethics

Some of us sold our souls, ideas, skills, imaginations: maybe to pay the rent when the bubble of technological creativity burst and the cool and morally easy jobs became scarce. We sold our head to corporations or the government to build the kind of things we knew perfectly well how to build, things that we had sometimes discussed as an intellectual game, never intending to make them a reality. Like surveillance infrastructure. Like software to analyse camera images in real-time for movement patterns, faces, licence plates. Like data mining to combine vast amounts of information into graphs of relations and behaviour. Like interception systems to record and analyse every single phone call, e-mail, mouse-click in the web. The means to track every single movement of people and things.

Understanding what uses one's work can be put to is one thing. Refusing to do particular work because it could be put to use in ways that cause harm to other people is something else entirely. Especially when there is no other good option with regard to earn a living in a mentally stimulating way. For those of us caught in this dilemma, most projects by themselves were justifiable, of course. It was not that bad or no real risk. Often the excuse was, "it is not technically feasible today anyway, it's too much data to store or make sense of". Ten years later it is feasible. For sure.

While it certainly would be better if the surveillance industry died from a lack of creative minds within it, the more realistic approach is to keep talking to those of us who have sold our heads. We need to generate a culture that might be compared with the sale of indulgences in the earlier dark ages: you may be working on the wrong side of the

barricade, but we would be willing to trade you private moral absolutism in exchange for knowledge. Tell us what is happening there, what the capabilities are, what the plans are, which gross scandals have been hidden. To be honest, there is very little that we know about the capabilities of today's dark-side interception systems, following the initiation of the Echelon system.² All the new surveillance technology that monitors the internet, the current and future use of database profiling, automated CCTV analysis, behaviour pattern discovery and so on, is only known in very few cases and as vague outlines.

We also need to know how the intelligence agencies work today. It is of highest priority to learn how the *we-would-rather-use-backdoors-than-waste-time-cracking-your-keys* methods work in practice on a large scale, and what backdoors (methods of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection) have been intentionally built into or left inside our systems. Building clean systems will be rather difficult, given the multitude of options to produce a backdoor ; ranging from operating systems and application software to hardware and CPUs that are too complex to audit fully. Open Source does only help in theory, and who has the time to really audit all the sources, anyway^a

Of course, the risk of publishing this kind of knowledge is high, especially for those on the dark side. So we need to build structures that can reduce the risk. We need anonymous submission systems for documents, methods to clean out eventual document fingerprinting (both paper and electronic). And of course, we need to develop means to identify the inevitable disinformation that will also be fed through these channels to confuse us.

Building Technology to Preserve the Options for Change

Today we are facing a unprecedented onslaught of surveillance technology. The debate whether this may or may not reduce crime or terrorism is no longer relevant. The *de facto* impact on society can already be felt with the content mafia (a.k.a. RIAA, the Recording Industry Association of America)³ demanding access to all data to preserve their dead business model. We will need to build technology to preserve the freedom of speech, the freedom of thought, the freedom of communication. There is no other long-term solution. Political barriers to total surveillance have a very limited half-life period.

The universal acceptance of electronic communication systems has been of tremendous help to political movements. It has become a bit more difficult and costly for those in power to keep their secrets. Unfortunately, the same condition applies to everybody else. So one thing that we can do to help society's progress is to provide tools, knowledge and training for secure communications to every political and social movement that shares at least some of our ideals. We should not be too narrow here in choosing our friends. Everyone who opposes centralistic power structures and totalitarianism should be welcome. Maintaining political breathing spaces becomes as crucial as the utilisation of the space for specific ends.

Digital anonymity will become the most precious experience. Encrypting communications is convenient and necessary, but does not really protect one's privacy or

identity. Traffic analysis is the most valuable intelligence tool around. Only by automatically looking at communications and movement patterns can the interesting individuals be selected, those who justify the cost of detailed surveillance. The widespread implementation of anonymity technologies becomes seriously urgent, given the data retention laws that have been passed in the European Union. We need opportunistic anonymity in exactly the same way as we needed opportunistic encryption. Currently, every anonymisation technology that has been deployed is instantly overwhelmed with file-sharing content. We need solutions for that, preferably with systems that can withstand the load, as anonymity loves company and more traffic means less probability of de-anonymisation by all kinds of attack.

Closed user groups have already gained momentum in communities that have a heightened awareness and demand for privacy. The darker parts of the hacker community and a lot of the warez⁴ trading circles have gone black already. Others will follow. The technology to build real-world, working, closed user groups has yet to be developed. We have only improvised setups that work under very specific circumstances. Generic, easy-to-use technology to create fully encrypted closed user groups for all kinds of content, with a comfortable degree of anonymity, is desperately needed.

Decentralised infrastructure is the need of the hour. The peer-to-peer networks are a good example, if one wants to see what works and what not. As long as there are centralised elements, they can be taken down under one pretext or another. Only true peer-to-peer systems that need as few centralised elements as possible can survive. Interestingly, tactical military networks have the same requirements. We need to borrow from them, just as they borrow from commercial and open source technology.

Designing technology that is able to counter surveillance abuse is the next logical step. A lot of us are involved in designing and implementing systems that can be put to exactly this use. Be it webshop systems, databases, RFID (Radio Frequency Identification) systems, communication systems or ordinary Blog servers, the design should be able to protect the system against later abuse of collected data or interception. Often there is considerable freedom to design within the limits of our day jobs. We need to use this freedom to build systems in a way that they collect as little data as possible, use encryption and provide anonymity as much as possible. We need to create a culture around this principle. A system design needs to be viewed by our peers as good only if it adheres to these criteria.

Of course, it may be hard to sacrifice the personal power that comes with access to juicy data. But keep in mind, you will not have this job forever, and whoever takes over the system is most likely not as privacy-minded as you are. Limiting the amount of data gathered on people involved in everyday transactions and communications is an absolute must if you are a serious hacker. There are many positive features of RFID: for instance, making the recycling of goods easier and more effective, by storing information about the material composition and hints about the manufacturing process in tags attached to electronic gadgets. But to be able to harness the good potential of such technologies, the system needs to limit or prevent the downside as much as possible ; intentionally, not as an afterthought.

Do not compromise your friends with stupidity, or the impulse of self-protection will become even more essential. We are all used to the minor fuckups of encrypted mail being forwarded unencrypted, of being careless about other people's data traces, or bragging with knowledge obtained in confidence. This is no longer possible. We are facing an enemy that is euphemistically called *Global Observer* in research papers. This is a literal term. You can no longer rely on information or communication being overlooked or hidden in the noise. Everything is on file. Forever. And it *can* and *will* be used against you. And your innocent slip-up of five years ago might today compromise someone close to you.

Keep silent and enjoy, or publish immediately may become the new mantras for security researchers. Submitting security problems to the manufacturers provides the intelligence agencies with a long period in which they can and will use the problem to attack systems and implant backdoors. It is well known that backdoors are the way around encryption, and that all big manufacturers have an agreement with the respective intelligence agencies of their countries to hand over valuable 0-day⁵ data as soon as this becomes available. This way, the agencies can remain undetected for years without risking exposure. If by chance they are detected, no one will suspect foul play, as the manufacturers will provide the necessary explanatory rationales. So if you discover problems, publish at least enough information to enable people to detect an intrusion before submitting to the manufacturer.

Most important: have fun! The eavesdropping people must be laughed at, as their job is silly, boring, and ethically the worst thing to earn money with. We need to develop a *let's-have-fun-confusing-their-systems* culture that plays with the inherent imperfections, loopholes, systematic problems and interpretation errors that are inevitable with large scale surveillance. Artists are the right people to implement this kind of approach. We need a subculture of *In your face, peeping Tom*^a Exposing surveillance logic and methodology in a manner that reveals these to be degrading practices, and giving people something to laugh about with regard to it, must be the goal. Also, this prevents us from becoming frustrated and tired. If we don't enjoy taking on the system, we will get tired of the contest, withdraw from it; and they will win. So instead of being angry, ideological and obdurate, let's be funny, flexible and creative^a

A version of this text was first published under a Creative Commons licence in the journal *Die Datenschleuder*, # 89 (December 2005). <http://ds.ccc.de>

A forum to debate this text can be found at the author's weblog at http://frank.geekheim.de/?page_id=128

NOTES

1. The Clipper chip, suggested in 1993, was a cryptographic device intended to protect private communications while at the same time permitting US government agents to obtain the keys to this material upon presentation of what was vaguely characterised as legal authorisation. The keys were to be held by the government under terms of escrow, which would enable agents to access encrypted private

communication. The Clipper chip did not receive support from consumers and manufacturers, and the chip itself was a dead issue by 1996. See http://en.wikipedia.org/wiki/Clipper_chip

For the views of cryptography and computer professionals who opposed the Clipper proposal, see <http://www.cpsr.org/prevsite/program/clipper/clipper.html>

For an official statement by the US government on the Clipper chip, see http://www.epic.org/crypto/clipper/white_house_factsheet.html

2. In a massive international surveillance effort, the US National Security Agency (NSA) has created a global spy system, codename Echelon, to capture and process all satellite, microwave, cellular and fibre-optic communications traffic. Analysts at intercept stations maintain separate keyword lists for the purpose of analysing any conversation or document flagged by the system.

For a detailed history of Echelon, see <http://home.hiwaay.net/~pspoole/echelon.html>

For links, resources and media reports on Echelon, see <http://home.hiwaay.net/~pspoole/echres.html>

3. The RIAA is a critic of music file sharing, and has long contended that sharing of copyrighted music is a form of piracy, applying the well-known computing term to music. The RIAA especially targets music files uploaded onto the Internet using peer-to-peer software. It sees lawsuits as one way to combat the problem of internet-based piracy. See <http://en.wikipedia.org/wiki/RIAA>
4. The term *warezf* refers primarily to copyrighted material traded in violation of copyright law ; illegal releases by organised groups, as opposed to peer-to-peer file sharing between friends or large groups of people with similar interests. It usually does not refer to commercial for-profit software counterfeiting. The production and/or distribution of warez is illegal in most countries. However, it is typically overlooked in developing nations with weak or non-existent intellectual property protection. See <http://en.wikipedia.org/wiki/Warez>
5. Zero day or 0-dayf refers to software, videos, music or information released or obtained on the day of public release. Items obtained pre-release are deemed Negative dayf or sometimes -dayf. Zero-day software, videos, and music usually have been either illegally obtained or illegally copied. See endnote 3, RIAA; see also http://en.wikipedia.org/wiki/Zero_day

