基調講演 2公的問題と個人情報  現代社会におけるリスク、恐怖、安全、監視

<table>
<thead>
<tr>
<th>著者</th>
<th>原 佳美里 佐々木 恵雪 杏子 雪村 まゆみ</th>
</tr>
</thead>
<tbody>
<tr>
<td>雑誌名</td>
<td>先端社会研究</td>
</tr>
<tr>
<td>号</td>
<td>創刊号</td>
</tr>
<tr>
<td>発行年</td>
<td>2004年12月</td>
</tr>
<tr>
<td>ページ</td>
<td>321-355</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10236/11442">http://hdl.handle.net/10236/11442</a></td>
</tr>
</tbody>
</table>
Public Issues and Personal Information: Risk, Fear, Safety and Surveillance in Contemporary Societies

公的問題と個人情報
——現代社会におけるリスク、恐怖、安全、監視

David Lyon*
デイヴィッド・ライアン

訳：原佳央理**
林怡蓉**
雪村まゆみ**

2004 年度 第 2 回国際シンポジウム

「高度情報社会における危機管理
――安全性の向上か、それとも監視の強化か」

2004 年 9 月 20 日（月）
神戸国際会議場 国際会議室

*カナダ、クイーンズ大学（Queen’s University, Canada）
**関西学院大学
Public Issues and Personal Information:

Risk, Fear, Safety and Surveillance in Contemporary Societies

David Lyon

“Mina-san, konnichwa. O-isogashii naka, atsumatte kudasatte, arigatou gozaimasu.”

I’m going to make my comments in English and I hope that what I have to say will speak to the very important issues being studied within the special project through Kwansei Gakuin University: “Public Issues and Personal Information: Risk, Fear, Safety and Surveillance in Contemporary Societies.”

There is a Canadian singer, who, back in the early 1980s, wrote a song that is called “The Trouble With Normal.” And some of the lyrics from one verse are: “The person in the street” – the ordinary person in the street – “shrugs, ‘security comes first’.” But then the song goes on: “The trouble with normal is it only gets worse.” And it’s interesting that this was written at the time of the Cold War because it could easily be written in 2004. What is today seen by many people as a “normal” situation has actually taken the form of a very abnormal situation: the so-called “war on terror.”

It is abnormal in the sense that extraordinary measures are being called upon to combat this shadowy enemy of “the terrorist.” So on the one hand, we have extraordinary measures; on the other hand, we have a situation seen as “normal.” And what I have to say illustrates what the Canadian songwriter, Bruce Cockburn, was saying when he said that “The trouble with normal is it only gets worse.”

When the great American sociologist C. Wright Mills introduced students to his discipline, he stressed the difference between “public issues” and “personal information” − oh, sorry: “personal troubles.” And at that time, in the late 1950s, he had in mind questions of unemployment and matters like that that cause a lot of individual distress − and against which people feel helpless.

Today, old fears about unemployment or poverty have not gone away.
Rather, they have been joined by other fears about street safety, about travel security, about the reliability of computer-based communications. Uncertainties and anxieties seem to proliferate rather than diminish in information societies.

But just as in the day of C. Wright Mills, in the middle of the last century, many people individualize their “personal troubles.” Mills was trying to encourage people to put them in a bigger historical and social frame. Unemployment and poverty can be felt devastatingly on a personal level. But they are also structural problems within contemporary societies. The so-called information society tends to perpetuate the same kind of individualism that was present in C. Wright Mills’ day. And it does so especially through its dependence on gathering and processing personal data in every sphere of social life.

The quest of surveillance is for ever more unique identifiers by which people can be traced, tracked and monitored. Of course, people have always been placed in categories: We were placed in categories by our class positions, which heightened or lowered our risks of being unemployed. But now, the categories are more varied but less visible because they are within electronic systems.

If C. Wright Mills was writing today I think that he would try to explicate the connections between “public issues” — the structural world of political economy and society — and “personal information” or personal data. And I think that he would try to show how the outcomes are still not inevitable and how alternatives are still available. And I think that he would be even more concerned to examine the historical origins of these information questions in their large social context in order to counter what I would say is the obsession with what might happen in the future, which plays such a large part today in risk management, security and surveillance.

So let me make a few comments about personal information as a public issue.

Personal information has become a public issue. We’re aware that in countries around the world, information has become something that is discussed
politically, whether it has to do with intellectual property, the governance of the Internet or in whatever other context. And indeed, a number of governments have over the past 30 years passed laws that relate to personal data, either as data protection laws or privacy laws or, in the case of Japan, the Personal Information Protection Act of 2003. So there is already a context in which personal information has become a public issue. And as you can hear, because I’ve connected it with the past 30 years, it has a lot to do with computerization.

The idea is to try to reduce the opportunities for abuse and to reduce the chances of error within data-handling regimes. But these issues are still very controversial. Many agencies that handle personal data regard the rules and laws as unnecessary — or worse, as a hindrance to the smooth running of the organization, which they say depends on processing as much personal data as possible. On the other side, many worry about the loss of personal liberty and privacy in the routine ways in which people’s life-chances are negatively affected by their so-called data-image.

Let me just stress that point. Much of what goes on in data protection and privacy law has to do with abuses: criminal activity, fraud. I want to suggest there is another area, which is the routine use of personal data, which may also have within it some very significant problems. But it is important to place in an historical and social and comparative context ways in which personal information has become a public issue — and to show why it deserves a much higher profile than it currently has.

Many years ago, details about personal identity — family name, age, gender, place of residence, work, income — stayed fairly close to the person. Today, as what we call governance is distributed throughout all social spheres, personal information is central to that process. Those apparently trivial personal details about gender and age and so on are now pivotal for social organization and the life-chances of citizens, workers, consumers, travelers — and you could probably mention a list of other types of role. And you might wonder why I don’t include the word “offender” within that list [or] “lawbreaker.” That’s because many of things that once applied in the area of criminal justice are now applied across all these areas: travel, citizenship and so on.
No citizens can be unaware of the increased use of electronic equipment in attempting to stabilize identities, especially at national borders — and especially after 9/11. But even if full-scale national identification card systems, like the Juki system here in Japan, even if they’re not in place, most of the advanced societies are moving towards biometric standards into passports — a process that has accelerated since 9/11. But then, employees are also aware of new ways in which their work is being monitored: checking their times, their location, using entry cards, automated keystroke counting or location devices in vehicles and telephones.

Consumers are also subject to an array of technologies designed to encourage them to purchase goods and services, from supermarket loyalty cards to database marketing, all of which rely on the garnering of personal information in order to create customer profiles.

In any era of unprecedented mobility — traveling across borders, especially, but also within national borders — aspects of travel also come under scrutiny. Travelers may expect to be located routinely for policing and also for commercial purposes, both by fixed technologies such as closed-circuit television or video surveillance, or mobile ones such as cell phones or in-car navigation systems.

There’s a sense in which, as identification cards and other similar items are used, that the old notion of a fixed border around a geographical area is less important. The border becomes virtual; the border is everywhere. And so travelers may all the time be subject to the possibility of checks.

This means that governance in general is being decentralized and dispersed, especially as it relies more and more on these little checks, on these little controls, at every point. It contributes to what you might call social discipline and order, but it also contributes to a society based on controls — these little “protocols” that we have to confront every day.

However, we cannot understand personal information as a public issue and the development of societies of control without saying something as well about “risk.”
In recent decades a lot has been made of the question of “risk” in contemporary societies. Ulrich Beck, a German writer in sociology, sees risk as a response to industrialism — particularly, obvious environmental threats from the uninhibited use of certain kinds of industrial techniques. But today the category of “risk” has been taken far beyond the immediate area around nuclear power stations or leeching out of landfill sites of toxic materials. It has been taken into many other areas too, including, of course — notoriously since 9/11, particularly — “terrorism.” Since then, security, which was already growing in importance politically since the Second World War, has become a predominant political preoccupation.

And it relates to risk. Security has been dominating the American election campaign over the past few weeks. And still it does now. The question of how to respond to the report on the investigation into 9/11 is what the candidates are using all the time in the political debate. It was also central, of course, for the Summer Olympics in Athens this year. No less than two billion American dollars were spent on security for the games in Athens. The dream of peaceful cooperation and competition between nations has also become a test site for surveillance technologies. And of course, this didn’t begin after 9/11. It began after the 1976 — sorry, the 1972 — Olympics in Munich, when members of the Israeli team were killed. But nonetheless, security has become central to the Olympic operation.

And it illustrates a very important point about risk that I want to stress, which is that although the security set up for the Olympics is a response to threat and risk perceived by the organizers — and actually demanded by the United States — the ways in which security is set up itself then creates further risks, as many of the citizens of Athens who protested against the security devices were to argue.

And this is because those citizens rightly noted that once security and surveillance equipment is in place, once the money has been spent and the infrastructure has been built, it is very difficult to dismantle. The tendency in the setting up of any security and surveillance system is not then to reduce that system, but to enhance it and, indeed, to use it for other purposes as well as
those for which it was originally intended. And one could bring plenty of empirical evidence to show that that has been the case over the last few decades.

So what do we mean about this question of risk? It is, as it were, the “dark side” of modernization. And a focus on risk means that the world is conceived, is thought of, as hazardous, as dangerous. The risks can be external, such as natural disasters — earthquakes being a very obvious case in this part of the world — but it can also be technological failures or threatening behaviors of groups or individuals. They can also be internal, such as viruses that lurk in the body or, of course, within the body politic: the notion of “enemies within” a nation-state perceived to be a risk. Either way, the emphasis is on that “dark side” of modernization.

Ulrich Beck’s work suggests that risks multiply themselves, they proliferate, they breed, as it were, in global modern societies — and that this is made worse, its impact is exacerbated, by the general deregulation of economy and society since the 1980s. The result of that is that just as the risks seem to be more and more threatening — shadowy, unknown, unpredictable risks — just at the time when the risks seem to be increasing, so individual lives seem to be more on their own. Individuals feel alone in an apparently threatening world.

Current notions of “security” in response to risk have a lot to do with what we’ve been describing as “terrorist” threats, but it’s important to note that there is a continuity here. Although many commentators said everything changed after 9/11, anyone with any sense of history will realize that there is huge continuity between the strategies and tactics applied before and after 9/11. What 9/11 did was to give a rationale and a pretext for the reinforcement and the amplification of security and surveillance. It did not lead to its invention for the first time.

Within risk societies, then, risk is related to governance, which has to do with the provision of security. By “governance,” I mean what happens in the realms of power in many areas of life — not just governance by the state, although it must be said that the state still plays a very important role within
governance. I’m certainly not one who believes that the state is withering away in the 21st century.

And the nation-state is now centrally concerned with the provision of security, which in turn has become an economic category. The OECD now has a new category of industry called the “security industries.” So, any new surveillance technologies refer to that kind of risk-society analysis.

Risks were a key to developing forms of criminology during the 20th century. But many of the categories that once applied to offenders, lawbreakers, are now being transferred to national security. The French thinker Jacques Ellul once said that in order to apprehend criminals, everyone has to be supervised. He said that in 1964. In 2004, we could simply change one word and say: “In order to apprehend terrorists, everyone must be supervised.”

So the quest for security drives the need for surveillance. We need knowledge, we need information, to be communicated so that we know what the risks are. That is how the argument runs. And surveillance methods of the most advanced kind are required for this — so it is argued. One of the key examples that I have already mentioned is the idea of national identification cards like the Juki-Net system, like systems that are already more advanced than that in Malaysia, Hong Kong, Thailand, Singapore — and are, in fact, already being tested in countries like India and China. There’s a proposal in Britain now before the British parliament this fall to create a national ID card system. And this makes a good, concrete example of what I’m talking about.

The ID card being proposed in Britain has a biometric identifier within it, probably an iris scan across the eye. And in line with what I’ve been saying, those cards, whatever their contribution to security, will also carry risks of their own.

On the one hand, the cards themselves can do very little to minimize a security threat from guerrilla activity or terrorist activity. Why not? Well, for a number of reasons: the limitations of the biometrics, the reliance of the documents on other kinds of document, like birth certificates, and the fact that to work properly, you would need to have personal data within the database about terrorist suspects; otherwise, you couldn’t actually create a system based
on identification cards that would be useful against terrorism.

But on the other hand, there are other kinds of risks, not just that the card won’t work — but that it will work for other purposes. Because they end up being general population management tools and, as has been argued by a number of authors, in the places where they are being set up and proposed, it is often those who are in “marginal” and “vulnerable” positions who are negatively affected by the implementation of such card systems.

So as I say, the idea of an ID card, a national card based on a national registry using biometric methods, is one other way in which, as I say, risks are reproduced; new risks may be generated. And those risks have to be considered by anyone concerned with setting up security systems.

You could say that in the demand for information, risk is a central feature. Risk management drives the quest for more surveillance data, so that you can assess risks, set up threat levels, and so on. If that’s the demand side for surveillance information, the supply side comes in part from fear.

That is to say, those populations and population segments that exhibit higher levels of fear will also be those who are more willing to provide the surveillance data. So supply of surveillance data — in this case, personal data — is encouraged by “cultures of fear.” Risk helps us understand the demand side; fear helps us understand the supply side.

Of course, there are many, many other things we could talk about this afternoon. I think that there are other things as well as fear that help on the supply side. There is evidence of much complacency and even welcoming of surveillance measures by some populations. And I think this has a lot to do with contemporary popular culture: It has to do with the role of the mass media; it has to do with “McDonaldization” and “Disney-ization” of contemporary societies.

I’m not going to argue about all those, but I just want to make this point about fear: There are many “cultures of fear” in the 21st century. I don’t take the view that there is a “culture of fear” that is somehow rolling across the world. But I do believe that there are many cultures of fear that have become
more significant in the last 10, 15 years — and this, again, has been amplified since 9/11.

The fears range from very local ones — parents who no longer allow their children to walk to school and prefer to take them in cars because they fear what we call “stranger danger” — right through to the fears that I was mentioning a moment ago: unpredictable fears about unknown threats “out there.” Not just terrorism. Things like climate change, global warming, the possibility of natural disasters; all these things are significant within these cultures of fear. So they occur at every level.

On a societal level, especially since 9/11, certain groups have been seen as productive of fear, those “enemies within” that are suspected — and of course, they nearly always have stereotypical Middle Eastern/Arab/Muslim characteristics. These racialized characteristics have become very common and they have led to the suspension of many civil rights since 9/11, and this includes the suspension of those rights through the development of new surveillance technologies that create categories of suspicion.

Fears have been fanned by the establishment of security departments or departments of homeland security, like the one in the United States, and the constant admonition to ordinary citizens to become the “eyes and ears” of the security forces. Such “eyes and ears” are intended to work in conjunction with fully fledged systems of intelligence and surveillance, who today have such huge and rapidly growing budgets.

But once again, the very presence of armed guards, signs of surveillance, warnings about the possibility of surveillance, tends to reinforce and reproduce fears. So, fear feeds on fear. Signs of security breed a sense of insecurity.

But of course, as the third point there says, fear is unevenly distributed and, in fact, unrelated very often to statistical facts about safety levels. People appear to be most fearful of things that are far beyond their control. Thus, after 9/11 many chose to drive rather than fly, even though statistically it is far more dangerous to drive on highways than it is to fly. Women believe that they have a greater chance than men of being hurt in a terrorist attack, even though the risks to women and men appear to be quite even. People tend to overestimate
risks, and to lean towards worst-case scenarios, as well as to respond more readily to images than to arguments.

So it is that those fateful pictures of the burning and crumbling Twin Towers *must be* the most influential images of the last four years on a global level. They reinforce the notion of risk and, simultaneously, reinforce fears. And therefore, people, because they are fearful, will go along with new measures, even when they seem to create further problems. Think, for example, of the longer time that we have to wait in line in airports. We accept inconvenience because we believe somehow that because of it, we are more safe.

So fear is unevenly distributed, unrelated to statistical facts about safety levels. But it also helps to galvanize political responses to minimize risk—but, I would argue, that are also repressive.

In so-called risk societies, measures to guarantee safety proliferate as never before. The “bads,” as opposed to the “goods,” of industrial production, have to be contained or countered: People require protection from radiation emitted by nuclear power plants or toxins leeching out of landfill waste sites. Seatbelts have to be worn in cars to reduce injuries in road accidents. Buildings have to conform to codes ensuring their capacity to withstand earthquakes or to keep breathable air circulating.

So it’s hardly surprising that with media-amplified threats to security from “terrorism” following some spectacular, and spectacularly deadly, surprise attacks, the demand for security and safety rise even more sharply. They have become top priorities politically, even eclipsing some civil rights and liberties that were, until recently, hallmarks of some advanced democratic societies.

Now, I’m referring to “safety” in this section, partly because the notion of “security” has other connotations. In the era of the welfare state, “security” was usually thought of in welfare, in social terms, rather than in national and military terms. And therefore, it could be confusing to think about “security,” as if that which related to state welfare was the same as what we’re talking about today.
Today’s “security” is all about making streets, airports and cities safe from accident and especially from malevolent people, often thought of as “terrorists,” although, of course, the category of “terrorist” has also expanded. In the example of the Olympic Games in Athens, it turns out that the security forces were concerned about a bundle of threats, including anti-globalization groups, Middle Eastern “terrorists” and also local citizens who spray-painted the CCTV cameras to blur the vision through the lens.

The preferred way of trying to achieve safety is technological. This has become increasingly clear in the past few years. It is, if you like, a technical “fix” which is sought. And so this invites a political economy discussion of security and also one that relates to cultural dependence on technology.

Why would we seek technological solutions for what are political and social problems? Well, they’re very good questions. There has been a search, as I say, within the contemporary governments for new security systems to be provided by the security industries. But at the same time, ordinary commercial operations may be brought in to supplement the publicly provided security.

In the United States, the developing situation is now so pronounced that it is described as the “security-industrial complex” by the American Civil Liberties Union. “Privatized surveillance” is encouraged alongside public surveillance.

But how far is all this activity justified? Is “safety” really safe? Can we have too much security? Well, what a strange question, you might say, when we’re supposed to be discussing the significance of security and risk and so on in the 21st century. Surely security is the only thing that we need. It is the “good thing” above all; how can you have too much of a good thing?

I think we can argue that there are real questions about security and safety as an unqualified “good thing.” This is a “black box” that has to be opened to see what is inside it. Are we assuming the “normal” once again, and forgetting that it can “get worse”? Lucia Zedner at Oxford University in England has argued that much “security” is actually paradoxical. For example, it presumes that threats will persist, even though it tries to reduce risk. “Security” also promises reassurance but, at the same time, as I’ve been arguing, increases
anxieties.

Again, it is supposed to be a universal good: “Security is good for everyone.” But actually, the means of security that we are seeking, particularly those that use surveillance, is based on exclusion. How can that be a universal good? Again, it promises freedom, while at the same time eroding civil liberties.

In all these ways, then, it’s possible to have too much of a good thing. The paradoxes of security and safety need to be explored, interrogated, examined. And they need to be publicly debated. This is something that is a central area for democratic participation in the 21st century.

Well, the chairperson promised that I would say something about surveillance, and I’ve said several things obliquely about surveillance. Let me just make a few comments, as I come towards to the end of my remarks, about surveillance.

Surveillance is an ancient technique. It is something that is as old as history. Today it is technologically enhanced. In the earlier part of modernity it was bureaucratically enhanced; now it is computer-assisted. So it’s not the product of new technologies, neither is it the response to 9/11. It’s a much more long-term process that we’re looking at.

I understand surveillance, the second point on the screen, as focused attention to personal details, for the purposes of management or control or influence. And therefore, the way that I understand it, it is always ambiguous. Just as in the language from which this word comes, French, the verb surveillier is ambiguous, so I think all surveillance is ambiguous.

Think for a moment about the welfare state to which I have referred already. In order to create an effective welfare state where no member of a given society is left out, is pushed to the margins just because they are poor or sick or unemployed, in a welfare state the system depends upon collecting and processing personal data — to ensure that those who are most vulnerable will, in fact, receive the benefits that they need to get. You need surveillance for that situation. And who is going to argue against a system that protects the most
vulnerable members of a society?

So, do you see what I’m saying? It’s always ambiguous. The ambiguity in French has to do with “watching over,” to care for someone — if I watch over a child, for example — and watching over to check that someone is doing something or is not doing something. The manager in the corporation who is “watching over” to check that I am working at a particular pace or doing the things that I’m expected to do. That is surveillance for control and management; the other is surveillance for care.

So I think there’s always an ambiguity here, and it’s dangerous for us simply to talk about surveillance as a negative feature of contemporary societies, as some do.

That does not mean, of course, that there are not some great dangers in surveillance today, and I think it’s one of the most critical issues confronting contemporary societies, especially since 9/11 — because the pendulum has swung, and is swinging, very strongly from surveillance as any kind of care through to surveillance as control. Anyway, that’s the way that I think we can understand surveillance.

And I was talking a few minutes ago about surveillance in its routine use rather than in its criminal or abusive aspects. In its routine use, surveillance is intended to sort between different categories of people and to deliver different kinds of treatments or outcomes to those different groups that have been sorted. Insurance is an obvious case in point.

So it’s future-oriented; it relates to what might happen in the future rather than necessarily on past records. It relates to what can be found in abstract data rather than on what people say, what their own stories are. And increasingly, it is to prevent threats from being fulfilled. It is a tool of governance that is both flexible and fluid.

Let me make some concluding comments.

The “war on terror” that gives a lot of the context to things that we’re discussing today has no enemy. What is “terrorism”? What is a “terrorist”? To declare “war on terrorism” is like declaring war on carpentry or yoga: It’s a
tactic, it’s technique. It isn’t a movement or a thing. It’s also endless. Who is going to say when the so-called “terrorist threat” has come to an end?

Risks and fears, from what I’ve argued, spiral symbiotically. There’s a mixed metaphor there, but I think you know what I mean. There is a movement that is always spiraling upwards and it grows together: fear, risk, fear, risk, growing together. That’s what I’ve been arguing.

I’ve also been arguing that surveillance does not solve security problems. It may contribute to their partial solution — and don’t understand me as denying that for one moment. It doesn’t solve security problems, however, nor can it ever. But it does, at the same time, create some others. And no one can set up a system of surveillance and security responsibly without acknowledging and considering beforehand those other risks that are created by the attempt to minimize some already-existing risks. To do so, I suggest, is anti-social and is a denial of some of the basic understandings of democratic governance in the 21st century.

So in some ways, what I’ve been saying is that we have to check on the technical systems that we set up to try to meet risk and to provide security. That is one thing that I’ve been arguing.

We could also go beyond this, though, and from time to time ask whether we need the system at all — which would be a much more radical question to ask. If we did ask that question, then we might say: “Well, are there some other priorities that we could develop, like attempting to understand the roots of terrorism, discontent and violent activity emanating from some persons in Middle Eastern countries?” One might do well to ask: “How much effort after 9/11 has been devoted to trying to understand the roots of terror, rather than trying to create fortresses of technologically enhanced protection for the citizens of the rich countries of the world?”

Well, I started by quoting to you from a Canadian songwriter about “The trouble with normal is it only gets worse.” Well, clearly there’s a danger: If we accept all these new security and surveillance systems as “normal,” don’t let us imagine that they will remain “normal” without the possibility of their
getting worse. I’ve begun also to suggest that there may be ways of pointing to alternatives than this mere obsession with surveillance technologies and paradoxical security.

C. Wright Mills, whom I quoted also at the beginning, would also want to look at questions of alternatives. I’m not going to discuss them here, but they certainly come within the framework of the quest for human well-being, which is at the heart of the research project that gives us today’s symposium.

The opposing concepts to those that I’ve been talking about may act as signposts and as a way of thinking about alternatives. Risk makes little sense if there is no trust and mutual reliance. Fear only occurs when care and love are absent. Safety and security mean little without freedom, fairness and the means for human flourishing. At the end of the day, it is what these signposts point to that really matters.

“Arigatou gozaimasu.”