

GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation,
which can be downloaded from GISWatch.org



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Creative Commons Attribution 3.0 Licence <creativecommons.org/licenses/by-nc/3.0/>



Japan Computer Access for Empowerment

Hamada Tadahisa
www.jca.or.jp

Introduction

In 2012 the Japanese government passed legislation that presents a number of challenges for progressive civil society activists. Both the so-called Common Number Law and the State Secrets Protection Law reinforce surveillance regulations. Legislation is also pending that will expand the ability of authorities to “wiretap” the country’s citizens. These legislative changes can be seen as part of a process of the increased militarisation of the country, with startling parallels with changes in Japan ahead of World War II.

This new security legislation is far from fair, not only in terms of its content, but how it was developed. The bills were approved by the political majority without sufficient deliberations in parliament. The mass media also did not report on the controversial points before they were passed.

In this report we compare the legal frameworks governing communications surveillance today and those that existed before World War II in Japan. This is an attempt to learn the lessons of history so we do not repeat the mistakes we have made in the past.

Policy and political background

The Japanese government has been trying to develop laws that promote the control of information and surveillance for decades. It planned to introduce a national identification number in 1968, but every time it submitted the bill, the mass media strongly opposed it, and the attempts failed. Eventually, it managed to get the resident registry network bill passed, together with a wiretapping bill and bills related to defence cooperation, in 1999. At that time, the Japanese mass media did not report the deliberations in parliament sufficiently. Instead, they spent all their broadcasting time on a tabloid show: a verbal battle between Mitchy and Satchy, two on-screen women talents.

The government submitted the state secrecy bill in 1985, but failed to have it passed. It revised and submitted a bill on state secrets in 2013, and

managed to get the bill passed. The law is supposed to come into force in December this year – so this year might be one of the turning points in Japanese history. Moreover, a conspiracy bill and a revision of the Wiretapping Law are anticipated in 2014. This, together with the Common Number Law enacted in May 2013, suggests Japan is rapidly slipping into a paranoid surveillance state.

Here is a list of problematic legislation concerning communications surveillance:

- The Wiretapping Law (1999)
- The Computer Surveillance Law (Cyber Criminal Law) (2011)
- The Common Number Law (2013)
- The State Secrets Protection Law (2013).

Japan is one of 36 countries which international watchdog The Citizen Lab¹ shows used FinFisher, a notorious surveillance technology used to surveil internet users.

A tale of two Olympic games in Tokyo

We need to understand that the legislation promoting the regulation and control of information described above is part of a combined approach to legislative changes prepared over the past years, such as legislation defining the nation’s response to foreign military attack (2003) and an act dealing with the protection of citizens in the event of an armed attack (2004).

Many intellectuals have argued that the current situation in Japan closely resembles the situation before World War II. Because of this, we would briefly like to compare the run-up to two Tokyo Olympic Games, one scheduled for 2020, and the other in 1940, which was cancelled due to the war.

That Tokyo will host the 2020 Olympic Games is welcome news for many in the country. However, some people are concerned about the strengthening of the surveillance system for the games, and how this can be used to control citizens in the future.

During the Olympic Games held in London in 2012, the security and surveillance system used there became the centre of attention. The system included a network of CCTV cameras mounted

¹ <https://citizenlab.org>

throughout London, and unmanned aerial vehicles (UAVs), more commonly known as drones.

In 2014, the Tokyo Metropolitan Government started to install five security cameras for each elementary school zone – a target of 6,500 cameras to be installed by 2018. The total expenditure is expected to reach 2.47 billion yen (USD 25 million) over five years.

The 1940 Summer Olympics were originally scheduled to be held in Tokyo, 80 years before the Tokyo Olympic Games scheduled for 2020. However, they were cancelled due to the continuation of the Second Sino-Japanese War. The states of affairs before the two Olympic Games are remarkably alike:

- 1923 The Great Kanto Earthquake (A)
- 1929 The Great Depression (B)
- 1937 The Imperial General Headquarters² . . . (C)
- 1937 Complete revision of the Military Secrets Act (D)
- 1940 The cancelled Tokyo Olympics (E)
- 1941 The Pacific War

- 1995 The Great Hanshin-Awaji Earthquake . . . (A)
- 2008 The Great Recession (B)
- 2011 The Great East Japan Earthquake (A)
- 2013 The National Security Council (C)
- 2013 The State Secrets Protection Law (D)
- 2020 (scheduled) Tokyo Olympics (E)

If we put the series of events leading up to the two games in order as above, we can see how militarisation in Japan progressed (or, is progressing), affected both by government decisions and natural disasters.

The 26 February attempted coup and wiretapping

The greatest attempted coup d'état in modern Japanese history occurred on 26 February 1936. It recently became clear that widespread wiretapping occurred during this time, even though it was illegal under the Constitution of the Empire of Japan in those days.

In the attempted coup, a group of young Imperial Japanese Army (IJA) officers rose in revolt and killed a number of leaders in Japan. While they succeeded initially and were supported by officers associated with the Imperial Way Faction,³ Emperor Hirohito was furious with the rebels. The rebels surrendered on 29 February. This provided the basis for a purge of Imperial Way members from the military. It led to a “unity” cabinet and the end of political

parties by the Imperial Rule Assistance Association⁴ in 1940.

This may have accelerated the movement towards war. The Control Faction⁵ in the Army believed in a military solution to secure resources in Southeast Asia and Oceania. The Imperial Way, however, had focused first on national development rather than expansion. This approach might have led to economic cooperation with China, rather than war.

At least seven weeks before the coup began, the telephones of the masterminds behind the coup were intercepted by Ministry of Communications officials and the military police. Although this fact was kept secret, 20 wiretapping records were discovered in the broadcast centre at NHK, Japan's broadcasting corporation, in 1977. These were shared with the public in the documentary *Martial Instructions to Monitor Phones*, broadcasted on 26 February 1979.

According to a 2007 book by Seiichi Nakata,⁶ the director of the documentary, an extraordinary cabinet meeting held immediately after the outbreak of the coup decided on the wiretapping, even while recognising it as illegal under the Constitution of the Empire of Japan.⁷ However, it became clear that the wiretapping began seven weeks before the incident.⁸ In other words, the Ministry of Communications had been wiretapping without telling other cabinet members.

Moreover, the Imperial Way Faction is thought to have anticipated the possibility of a coup by young Imperial Way officers several years before the incident. In fact, Major Katakura and others wrote a document that served as an outline for countering a coup and using the subsequent repression to establish more political power.⁹ The “outline” includes detailed ideas and measures to be taken to reconstruct politics, diplomacy, defence, the economy, social policy and education, as well as how to manipulate public opinion. Many of these plans were realised by the Control Faction after the coup.¹⁰

The wiretapping records did not only infringe on privacy, but included identity theft and impersonation to falsely implicate someone.¹¹ For example, Kita Ikki, a national socialist intellectual who influenced the Imperial Way Faction, but was not directly

2 en.wikipedia.org/wiki/Imperial_General_Headquarters

3 en.wikipedia.org/wiki/Imperial_Way_Faction

4 en.wikipedia.org/wiki/Imperial_Rule_Assistance_Association

5 en.wikipedia.org/wiki/T%C5%8Dseiha

6 Nakata, S. (2007). *Wiretapping in February 26th Incident* [Tocho 2.26 Jiken]. Tokyo: Bungei Shunju.

7 *Ibid.*, p. 45-46.

8 *Ibid.*, p. 91.

9 *Ibid.*, p. 77.

10 *Ibid.*, p. 78.

11 *Ibid.*, p. 93.

involved in the coup, was sentenced to death as one of the coup participants, and shot five days later. In this case, there is a wiretapping recording made on 28 February of someone pretending to be Kita Ikki, who at that time was already in prison. The person was involved in a smear campaign to paint Kita as the mastermind behind the rebellion, foreseeing the possibility of the recording becoming evidence in court.¹²

What is the lesson that we can learn from these facts? Speaking directly, unchecked, authorities have the potential to corrupt endlessly and may drive society into a dangerous situation. Moreover, surveillance can be too powerful and paranoid, and can result in the fabrication of crimes, instead of assisting legitimate criminal investigation.

By comparing these two periods, we can learn lessons from history and how we should engage the new political administration on issues of communications surveillance and transparency.

The meaning of the surveillance in the present age

Now, if we turn back to today, we can easily see how the need for surveillance has spread into new terrain – including the mass surveillance of citizens online. In part this has prompted the need to revise the Wiretapping Law.

At the House of Councillors plenary session on 12 August 1999, the Wiretapping Law was passed by a majority vote, including the Liberal Democratic Party, the Liberal Party and the Komei Party, and was enforced in August 2000. Since then, the number of wiretapping investigations conducted is reported in parliament every year – it currently stands at about ten a year.

Although it is a legislator’s view that emails are also included under the definition of “communication” in the Wiretapping Law, no interception of emails has been reported in parliamentary reports.

However, it is possible to presume that an email delivered to a mail server has ended its “communication” legally, even if the user has not read the email. If so, emails may be confiscated without restriction through simple search and seizure or inspection.

Furthermore, it became possible to “seize” emails on a mail server from a remote personal computer or mobile phone after a Criminal Procedure Code revision.

The Legal System Investigation Commission is considering a revision of the Wiretapping Law. A reform bill is likely to be submitted to an

extraordinary session this autumn, or to an ordinary session of parliament next year. The following is being considered:

- Expanding the ability of authorities to carry out wiretapping.
- Abolishing the need for an employee of a communications company to be present, enabling authorities to intercept communications with a court order using encryption technology and a key.
- Allowing authorities to intercept conversations through “bugging”. The ability to bug a room or other location is a serious concern because all the conversations held in that location will be monitored, and it will become legal to break into a location such as a building and install the bugging devices.

Conclusions

We need to recognise that democracy in Japan is under critical pressure. The government and others create public anxiety, either to do with potential conflict with another country, or within the country, and surveillance is enhanced.

Moreover, many in the mass media have not sufficiently served as a watchdog over authorities or responded to the people’s right to know without yielding to pressure from authorities.

The internet, which we use every day, offers the possibility of sharing vital information and promoting a free way of thinking. However, regrettably, the internet itself also now serves as a tool for mass surveillance.

In particular, there is a huge risk in “big data”. It will be possible to identify an individual if data which looks harmless is collected in large quantities. Furthermore, when targeted at a specific individual, the possibility of this leading to a serious invasion of privacy is high.

It is not necessarily the case that Japan will slip into fascism again, but this could be the case, even if democracy has been established. Germany gave Hitler the post of chancellor under the Weimar Constitution. Once we have decided that we will never repeat the past, it is very important for us to learn how fascism rose before World War II.

The Japanese constitution declares: “We, the Japanese people, desire peace for all time and are deeply conscious of the high ideals controlling human relationships, and we have determined to preserve our security and existence, trusting in the justice and faith of the peace-loving peoples of the world.” Japan did not become involved in a war for 69 years after World War II, thanks to this pacifism.

¹² Ibid., p. 158-161.

Surveillance is engendered by distrust of others. If a fellow creature's mutual distrust and fear develop, war will break out. Human beings will not be able to survive if they cannot build a society based not on distrust and fear but on trust and cooperation.

Action steps

The following actions steps are suggested for Japan:

- Push for transparency in government.
- Establish a privacy commissioner system which is fully independent from the government.
- Advance democracy through the reform of the mass media, promoting alternative media and educating the public in media literacy.
- Abolish laws that aim to surveil and control people.
- Promote and campaign for privacy in communications.
- Conceive of a society based on trust and cooperation, not distrust and fear.