Appendix10: Translation of the Tokyo District Court's Judgment on January 15 2014

Country of jurisdiction: Japan
Court: Tokyo District Court
Division: Civil 41st Division
Judge: Masamitsu Shiseki (Presiding Judge)
Soichiro Shindo
Humiyasu Miyasaki
Date of Judgment: 15 January 2014
Case Number: Heisei 23 (2011) Wa (Civil Case) No.15750, Heisei 23 (2011) Wa (Civil Case) No.32072 and Heisei 24 (2012) Wa (Civil Case) No.3266

Judgment

Main Text

1. The defendant Tokyo metropolitan government shall pay to each plaintiff, with the exception of plaintiff 4, money in the amount of 5.5 million yen as well as money accruing therefrom at an annual interest rate of 5% during a period starting from 26 July 2011 up to a date when the payment will be completed.
2. The defendant Tokyo metropolitan government shall pay to plaintiff 4 money in the amount of 2.2 million yen as well as money accruing therefrom at an annual interest rate of 5% during a period starting from 26 July 2011 up to a date when the payment will be completed.
3. The plaintiffs' other claims against the defendant Tokyo metropolitan government, as well as their claim against the defendant Japanese government, are dismissed.
4. The defendant Tokyo metropolitan government shall pay half of the plaintiffs' court costs and half of the defendant Tokyo metropolitan government's court costs, and the plaintiffs shall pay the remainder of the court costs incurred by the plaintiffs and the defendant Tokyo metropolitan government, as well as the defendant Japanese government's court costs.
5. Only the preceding paragraphs 1 and 2 can be provisionally executed in the present judgment.

Facts and Reasons

I. Claims

The defendants shall jointly pay to each plaintiff 11 million yen as well as money accruing

therefrom at an annual interest rate of 5% during a period starting from 26 July 2011 up to a date when the payment will be completed.

II. Outline of the Facts

1. In this case, the plaintiffs, who are Muslims, submitted that The Metropolitan Police Department (MPD), as well as the National Police Agency (NPA) and the National Public Safety Commission (NPSC): (i)encroached upon the plaintiffs' constitutional rights including the freedom of religion through the surveillance of mosques etc., as well as collecting, storing and using personal information in a manner that violates the Protection of Personal Information Held by Administrative Agencies Act (hereinafter referred to as the '**Protection Act**') as well as the Tokyo Metropolitan Ordinance for the Protection of Personal Information (hereinafter referred to as the '**Protection Ordinance**'); and (ii) subsequently, by breaching their duty of care etc. in information management, allowed the personal information to leak onto the Internet, and furthermore failed to take appropriate measures to mitigate the damage; both of which are illegal for the purposes of the State Compensation Act. The plaintiffs claimed damages of 11 million yen each, as well as money accruing therefrom at an annual interest rate of 5% during a period starting from 26 July 2011, the day after service, up to a date when the payment will be completed, against the defendant Tokyo metropolitan government, the entity liable for the Metropolitan Police Department, as well as the defendant Japanese government, the entity liable for the National Police Agency and the National Public Safety Commission.

2. **Undisputed Facts** (facts that are not in dispute between the parties, or readily follow the attached evidence or the pleadings in their entirety)

(1) **The plaintiffs**

The plaintiffs are all Muslims, and their nationalities are as follows.

Plaintiffs : Japan;

Plaintiffs : The Republic of Tunisia (hereinafter '**Tunisia**');

Plaintiffs : The Democratic People's Republic of Algeria (hereinafter '**Algeria**');

Plaintiffs : The Kingdom of Morocco (hereinafter '**Morocco**');

Plaintiff : The Islamic Republic of Iran (hereinafter '**Iran'**).

(2) **Occurrence of the Leak Incident**

On or around 28 October 2010, 114 articles of data (1 through 114 in Exhibit A-1, hereinafter referred to as '**the Data**') were posted on the Internet through the file exchange software Winny (Exhibits A-2 and A-3. Hereinafter this incident is referred to as the '**the Leak Incident**'.) As of 25 November 2010, the Data had been downloaded

onto more than 10,000 computers in over 20 countries and regions (Exhibit A-5).

(3) **Summary of the Plaintiffs' Descriptions in the Data**

In addition to numerous data regarding countermeasures against international terrorism, including a document marked "Outline for Reinforcing Reality Assessments" dated 10 September 2007, the Data contained A4- sized pages resembling résumés (hereinafter referred to as the '**Résumé-like Page**') with the nationality, birthplace, name, gender, date of birth (age), current address, place of employment and vehicle for each of the plaintiffs (with the exception of plaintiffs 1, 4, 13 and 17) and others. It also included information such as their date of entry, passport number and issue date, residence status, address at home country, duration of residence, registry date, municipality of residence and registration number (only the passport number, issue date and duration of residence for plaintiff 2) listed under the heading "Entry and Residence Related"; their history regarding residence address, schooling and employment in Japan under "History of Addresses, Schooling and Employment"; as well as e.g. height, build, and the presence or absence of hair, beard, or eyeglasses under "Physical Characteristics"; names, dates of birth, employers and addresses of family members, except for one individual outside this suit, under "Familial Relationships and Acquaintances"; and for some, the type, date obtained and number for their licenses under "Licenses'; date of arrest, offence, station of arrest and outcome under "Criminal Information"; as well as sections titled "Suspicions", "Response Status and Policy", "Affiliated Organisations", "Status, Positions and Roles etc.", "Comings and Going at Mosques", "Visited and Frequented Locations", "Summary of Behavioural Patterns", of which "Suspicions" and "Response and Policy" were recorded for all individuals, but other sections recorded for only some individuals, and with a profile picture attached (11(1) and (20), 1 (12) of Exhibit A-1).

Plaintiff 1's name, date of birth, employer and address was noted as the husband of plaintiff 2 under the "Familial Relationships and Acquaintances" section of the latter's Résumé-like Page, and plaintiff 4's name, date of birth and address was entered as the wife of plaintiff 3 under the same section of plaintiff 3's Résumé-like Page (11(5) and (14) of Exhibit A-1).

Although a Résumé-like Page for plaintiff 17 does not exist in the Data, the plaintiff's nationality, name, date of birth, passport number, residence status, employer and its address, place of birth, address at home country, address in Japan, mobile and home telephone numbers, family, entry and departure history in Japan and accessed mosques were recorded as "1 Particulars of Identity", together with a specific and detailed account of exchanges and friendship with a particular Muslim individual under "2 Information on Suspicions" (the document with the headings "1 Particulars of Identity"

and "2 Information on Suspicions" is hereinafter referred to as the '**Identity and Suspicions Page**').

Furthermore, although the Data did not include a Résumé-like Page or Identity and Suspicions Page for plaintiff 13, the surname of Plaintiff 13 appears under the "Suspicions" section on the Résumé-like Pages of plaintiffs 2, 3, 5, 7, 9, 11, 14 and 15 (11(3)-(5), (10), (11), (14), (15), (19) of Exhibit A-1) as well as under the heading "2 Information on Suspicions" in plaintiff 17's Identity and Suspicions Page (the plaintiffs' personal information contained in the Data are hereinafter referred to as the '**Personal Data**').

(4) **Investigation of the Leak Incident**

On 29 October 2010, the National Police Agency and the Metropolitan Police Department recognized the Leak Incident and commenced investigations.

The National Police Agency compiled interim findings etc. in December of that year, publishing a document titled "Regarding Interim Findings Etc. on the Case of Data about Countermeasures against International Terrorism Posted on the Internet" (Exhibit A-2), and on the 24th of that month the Metropolitan Police Department published a document titled "Regarding the Case of Data about Countermeasures against International Terrorism Posted on the Internet" (Exhibit A-3), comprising a summary of investigations thus far, etc. Each document mentions an acknowledgement of the fact that the Data contains information with a high probability of having been handled by a member of the police force, but does not disclose specifics of how the Data was removed.

Despite continued investigation by the police regarding the circumstances surrounding the posting of the Data, the details have not been revealed to this day (facts in the public knowledge).

3. Issues and Arguments from the Parties

(translation omitted)

III Judgment of this Court

(1) On Issue 1

(1) Regarding the Manner of Collection etc. of the Data

A) Taking into consideration (4) of the Undisputed Facts, the evidence (1 through 114, 2, 3 and 6 (1) of Exhibit A-1), and the pleadings in their entirety, it can be found that each of the documents that were the bases of the Data was in the possession of the Third Foreign Affairs Division [of the MPD].

B) Taking into consideration the Undisputed Facts, attached evidence and the pleadings in their entirety, the following facts can be found as the specific content of the Data.

a) A Résumé-like Page was created for the plaintiffs with the exception of A-C and 17, listing the items in (3) of the Undisputed Facts, including personal information on each of the plaintiffs including "Comings and Goings at Mosques" (save for plaintiff 12, whose comings and goings at mosques were not observed). As for the specific content of "Comings and Goings at Mosques", most individuals only had the name of the mosque they attend recorded, but it is stated that plaintiff 2 "instructs women and children in recitation of the Qur'an at Mosque D"; plaintiff E "participated in Friday prayers at Mosque F"; and plaintiff G "partook in Friday prayers and Saturday Arabic lessons at Mosque H, respectively, and these 3 plaintiffs are noted as taking part in religious ceremonies or instructional activities (11(2)-(5), (9)-(11), (14), (15), (18)-(20), and 1(12) of Exhibit A-1).

Notice has also been taken of many of the above plaintiffs regarding friendly relations etc. with a particular Muslim, in the "Suspicions" section of their Résumé-like Pages.

b) Regarding Plaintiff 17, although no Résumé-like Page exists in the Data, an Identity and Suspicions Page was created as per the Undisputed Facts (3). "J" is noted under the sub-heading "Mosque Accessed" in the "1 Particulars of Identity".

While Identity and Suspicions Pages were created not only for plaintiff 17 but also all plaintiffs other than 1, 4, 13 and 16, entries under its sub-heading "Mosque Accessed" did not differ significantly from entries under "Comings and Goings at Mosques" on the Résumé-like Pages. The "Information on Suspicions" section, in contrast, contains content that specifies and details the information under the "Suspicions" section on the Résumé-like Page. For example, regarding plaintiff 2, as well as the fact that she herself instructs women and children on recitation of the Qur'an, it is noted that plaintiff 1, her husband, holds a lecturer-like position at the mosque, is highly reputable as a Islamic lecturer, and consistently participates in workshops, special prayers, sermons etc., passionately engaging in missionary activities as a couple (15-18, 20, 21, 24-26, 29-31 of Exhibit A-1).

c) The fact that plaintiff 13's surname appears in the "Suspicions" section of the Résumé-like Page for plaintiffs 2, 3, 5, 7, 9, 11, 14 and 15, as well as under the "2 Information on Suspicions" sub-section of plaintiff 17's Identity and Suspicions Page, is as stated in (3) of the Undisputed Facts. Of those, in the "Suspicions" section for plaintiffs 2, 3, 5, 9, 11, 14 and 15, it is noted to the effect that they are or were acquaintances of plaintiff 13. In addition, on the Identity and Suspicions Page (19 of Exhibit A-1) of a Muslim individual outside this lawsuit, it is recorded as a result of direct questioning that said individual was asked by plaintiff 13 to deliver some cash, possibly terrorism funds, that was collected by the said plaintiff and sent it to another Muslim individual by hiding it inside an electric rice cooker; as well as the plaintiff's statement that despite *Jihad* obligations being waived due to heart complications, "I would go too, if needed"; as well as the name of plaintiff 13's wife and prefecture of residence.

d) That plaintiff 1 is plaintiff 2's, and plaintiff 4 is plaintiff 3's respective spouse, and that their names, dates of birth and such were recorded in the "Familial Relationships and Acquaintances" section of plaintiffs 2 and 3's Résumé-like Pages, is as stated in (3) of the Undisputed Facts. Also, plaintiff 1, as per above (b), was noted for his passionate missionary activities with his spouse in the Identity and Suspicions Page of plaintiff 2.

e) Further, considering the fact that the Résumé-like Pages created on the plaintiffs in above (a), (with the exception of plaintiff 16), (11(2)-(5), (9)-(11), (14), (15), (18)-(20) of Exhibit A-1), display a document date of 7 November 2008, and the Résumé-like Page created on plaintiff 16 (12 of Exhibit A-1) displays a document date of 2 October of the same year, and assuming that the Identity and Suspicions Pages, which are included in the Data just like the above Résumé-like Pages and share commonalities in their headings, were created around the same time, it can be found that the information in both the Résumé-like Pages and the Identity and Suspicions Pages were collected before November 2008, approximately.

C) Next to be considered are the circumstances of how each of the above information was obtained.

a) According to evidence (8 and 50 through 53 of Exhibit A-1) and the pleadings in their entirety, the Metropolitan Police Department was engaging in efforts to assess the state of Islamic communities at the risk of exploitation as terrorist infrastructure by November 2005 at the latest, said

efforts being undertaken at locations such as the Iranian Association, Arabic Islamic Institute, Tokyo Camii, Shin-Okubo Mosque, Otsuka Mosque, and Ikebukuro Mosque. The Metropolitan Police Department, in order to prevent international terrorism accompanying the Hokkaido Lake Toya Summit held from 7 July 2008 to the 9th of that month, had, since 23 June of that year, organised a "Mosque Squad" of 43 agents with the mission of "detecting suspicious activities of mosque attendants", designated K, L, M, N, O, P, Q and R mosques as "Mosques for Inspection", and for each of those mosques, stationed ground staff and behaviour-monitoring personnel from roughly 8:30 am, until the end of evening prayers at 7:30 pm, with the objective of detecting and observing new arrivals and suspicious individuals at the mosques. Of the plaintiffs on whom Résumé-like Pages were created (all plaintiffs with the exception of plaintiffs 1, 4, 13 and 17), their Résumé-like Pages, except for plaintiff 12, noted the name of the mosque they frequented as well as participation, if any, in religious ceremonies or instructional activities under "Comings and Goings at Mosques", as found in the above B (a); and the Identity and Suspicious Page created for plaintiff 17 listed Mosque J as "Mosque of Attendance" as found in the above B (b). In light of these facts, it can be assumed that for the plaintiffs, with the exception of plaintiff 12, information regarding their comings and goings at mosques and participation in religious ceremonies or instructional activities were collected by agents directly engaging in assessment activities (the monitoring of the plaintiffs regarding matters such as mosque access are hereinafter referred to as '**Mosque Monitoring Activities**').

Furthermore, the Metropolitan Police Department had been engaging in the collection of terrorism-related information etc. in cooperation with relevant agencies and businesses etc. (Exhibit C-1), and as it has been found that some of the plaintiffs had themselves been directly contacted or searched etc. (1, 2, 5, 7-9, 11, 13, 17 of Exhibit C-34), it can be assumed that the remainder of the information had been gathered through their receipt from relevant agencies such as the Immigration Bureau under the Ministry of Justice etc., or contacting and searching the plaintiffs as above.

b) Incidentally, the plaintiffs allege that the Metropolitan Police Department and the National Police Agency had, as of 31 May 2008, assessed and digitalised the personal information of "roughly 12,677 individuals"

equalling “roughly 89% of the 14,254 foreign nationals from Muslim countries registered in Tokyo”, and later, by the Hokkaido Toya Lake Summit convened July of that year, had “profiled roughly 72,000 individuals from OIC (Organisation of the Islamic Conference) countries (assessment rate of 98%)”, assessed the attendance of 3639 individuals by continuous surveillance at mosques, and conducted Information Gathering Activities regarding the names, locations, and financial situation etc. of Islamic-related organisations etc. However, in this lawsuit, the issue is simply whether or not the plaintiffs suffered damage through the illegal exertion of public authority carried out against them, so whatever information-gathering activities that may have been conducted in relation to Muslims and Islamic-related organisations other than the plaintiffs cannot be said to influence the judgment in this case.

In addition, the plaintiffs allege to the effect that the Metropolitan Police Department (i)established a relationship with 4 major automobile rental dealerships headquartered in Tokyo whereby they could receive user information without a referral document and had that information submitted; (ii)had hotels reinforce their retention of foreign passport photocopies; (iii)acquired the history of paycheck deposits for staff working at the Iranian embassy, from Tokyo Mitsubishi Bank (currently Mitsubishi Tokyo UFJ Bank); and (iv)obtained a roster of foreign students from the administrators at the Tokyo University of Agriculture and Technology as well the University of Electro-Communications, assessed the personal information of students from Muslim countries, and collected information on Muslims and Islamic-related organisations etc. However, there is inadequate evidence to find that the plaintiffs in this case had their information acquired by the Metropolitan Police Department through such methods.

c) Accordingly, it is fair to observe that the Data, by and large, was gathered in the manner of above (a).

D) On this point, the defendant Tokyo metropolitan government argues to the effect that the cause of action against said defendant is not identified with sufficient specificity, as the plaintiffs have not made individual and concrete arguments on the question of what measures and methods the Metropolitan Police Department officers employed in collecting particular personal information of the plaintiffs, instead alleging unconstitutionality in the relationship between the nationwide

police forces, including the Metropolitan Police Department, and all Muslims including the plaintiffs. The defendant Japanese government also argues to the effect that the plaintiffs' allegations are unfounded as it is unclear what breach of official duty they are alleging. Although it is true that the plaintiffs' allegations regarding the Information Gathering Activities contain sections that question the relationship *vis-a-vis* all Muslims including the plaintiffs, by redrawing this in terms of a relationship with the plaintiffs, it can be understood that they are arguing facts including the facts found and held in above (c). Considering that it is an undeniable fact that the plaintiffs' personal information was collected by police officers in one way or another, and that it may well impose hardship upon the plaintiffs to require precise identification of the measures and methods through which personal information of each individual plaintiff was gathered, the above degree adequately identifies the cause of action. Therefore, the defendants' foregoing arguments cannot be accepted.

(2) On whether the Information Gathering Activities violate the plaintiffs' freedom of religion under the Constitution (Article 20, Clause 1)

A) In light of the fact that the essence of the freedom of religion guaranteed under Article 20, Clause 1 of the Constitution is to preclude coercion by the State against sentiments and actions of believing in the existence of supernatural or superhuman beings and worshipping them in awe, it can be understood that prejudicial treatment in a legal or practical sense, or the existence of restrictive elements such as coercion, impediments or limitations, must be present in order to be able to say that one's freedom of religion was violated by the State. The Information Gathering Activities in the manner of above (1)iii were ultimately voluntary information gathering activities, not in themselves subjecting individuals to prejudicial treatment by reason of religious convictions, or imposing coercion, impediments or limitations in a religious way.

On this point, the plaintiffs allege to the effect that as the names of the plaintiffs' membership organisations and mosque of attendance etc. were particularised on the Résumé-like Pages, and as the objective substance of the Information Gathering Activities was to conjecture and identify individuals' faith, it thereby violated the freedom of religion. However, setting aside the fact that the State and public entities are banned from forcing individuals to profess their faith or demand proof of their faith, such as which religious organisation they are affiliated with, the information-gathering activities conducted to assess the plaintiffs' comings and goings at mosques merely involved agents going to the

mosques themselves and recording the plaintiffs' access from plainly observable external acts. In light of this mode taken by the Information Gathering Activities, it in itself did not possess an effect of coercion etc. against religion, as explained earlier. Therefore, it cannot be said that such activities come under the prohibition in relation to religious liberties. As a premise of the above allegation, the plaintiffs argue that the very attempt of State apparatuses to covertly conjecture individuals' faith is precluded in relation to the freedom of religion, but as explained below, the Information Gathering Activities were not conducted with the aim to conjecture individuals' faith. Therefore, it must be said that the plaintiffs' argument is unfounded.

The plaintiffs further allege that the Information Gathering Activities run the risk of labeling Islam as a religion that is not tolerated by society, thereby greatly prejudicing those who practice it. It is true that some of the plaintiffs, because of the information leak, were forced to resign from their occupation, or suffered economic loss by reasons such as a dramatic drop in sales at the stores they manage (6, 9, 10, 13 and 16 of Exhibit A-34). However, as these disadvantages were not due to the Information Gathering Activities themselves but the information in question leaking through the Incident, violations or restrictions on religious liberties by the Information Gathering Activities cannot be recognised based on the above disadvantages.

The plaintiffs further argue that it is understandable to hesitate from convening at the religious institutions in question under the circumstances of complete surveillance by the police, and that in reality, as seen in documents created by the police (51 of Exhibit A-1), the realisation that they were surveillance targets in the security measures etc. related to the Summit, which was implemented as a part of the surveillance of religious institutions, caused many Muslims to decline from attending mosques, with the effect of suppressing the prayers at the end of Ramadan, an important religious duty in Islam.

However, the above police document indicated by the plaintiffs (51 of Exhibit A-1) merely reports that worshippers during the 2008 Ramadan period increased drastically in comparison to the previous year, and that the cause may be attributed to Muslims in Japan, who had pulled back because of increased security in Tokyo incidental to the series of security measures related to the Hokkaido Toya Lake Summit, newly participating in religious services, in relief that no acts of terrorism in the name of Islam occurred in Japan during the Summit period. It does not note that worshippers during the 2007 Ramadan period decreased due to

police surveillance activities at religious institutions. Furthermore, the plaintiffs, at least in their arguments, have not articulated the degree to which they were aware of the Information Gathering Activities, particularly the Mosque Monitoring Activities. Moreover, their testimonies do not adequately support their cognisance of the Mosque Monitoring Activities. Plaintiffs 3, 5, 8, 11, 15 and 17 have testified that they saw police officers near the mosque they attended, with some testifying that they observed police officers entering the mosque. However, with the exception of one plaintiff who specified this as occurring after the Incident, the timing is unclear, and it cannot be determined whether they had noticed police officers before the Incident (24 (3), (5), (8), (11), (15), (17) of Exhibit A-3). While plaintiff 1 testifies of sensing on numerous occasions an atmosphere of surveillance at the S Institution, he has not testified to knowledge of the fact that the surveyors were police officers (34(1) of Exhibit A-1). What is more, none of these plaintiffs have testified of an actual chilling effect such as being effectively forced to cancel their participation in religious ceremonies at the mosques. As such, the plaintiffs' above arguments cannot be accepted.

B)

a) The plaintiffs allege that the Metropolitan Police Department, by a comprehensive surveillance of mosques targeting important religious ceremonies such as Friday prayers and Ramadan, discouraged Muslims from religious activities and suppressed attendance at mosques, violating the purpose of the Religious Corporations Act Article 84, which reflects Article 20 of the Constitution, and amounting to oppression and interference against the freedom of religion. However, there are inadequate grounds to hold that the plaintiffs were discouraged from religious activities or that attendance at the mosques were suppressed due to the Mosque Monitoring Activities, as recognised in Part i above, so this argument by the plaintiffs cannot be accepted either.

b) It cannot be denied that the timing of some plaintiffs' witnessing police officers around or inside the mosques they attend may have preceded the Incident. However, the plaintiffs are alleging to the effect that because the Metropolitan Police Department and the National Police Agency, under the name of counterterrorism, collected information exclusively on ordinary Muslims, the Information Gathering Activities were not a necessary gathering of information to prevent terrorist acts, instead amounting to oppression and interference against religious liberties. In view of the

significance of the freedom of religion as one of the constitutionally guaranteed freedoms of spirit, the court will also rule on this point for confirmation.

c) The Data contains expressions at various points suggesting that it was created as a countermeasure against international terrorism, such as entry to the effect that the assessment of the current situation surrounding persons from Muslim countries and Muslims in Japan is promoted as "countermeasures against international terrorism (4 of Exhibit A-1), and according to the attached evidence as well as the pleadings in their entirety, the following facts can be found in relation to international terrorism.

i. In general, 'terrorism' refers to acts such as the killing and harming of humans with the aim to coerce states etc. to accept etc. the specific cause or claim that forms its basis, or to intimidate etc. society (Exhibit B-3), and as of 31 July 2012, 49 organisations including so-called radical Islamic groups such as Al Qaeda, Hezbollah, Jemaah Islamiyah, and Lashkar-e Taiba, were designated by the United States government as foreign terrorist organisations that threaten the security of the American people or American national security (defence, foreign relations or economic interests) (1 and 2 of Exhibit B-38, and the totality of the pleadings).

ii. The following incidents of international terrorism had occurred before November 2008, when the Information Gathering Activities took place, just to raise some major recent examples.

(i) On 11 September 2001, simultaneous multiple terrorist attacks took place when 4 passenger aircrafts for US domestic flights were hijacked by 19 young Arab men acting under the orders of radical Islamists, of which 2 crashed into the World Trade Center buildings in New York, USA and 1 into the Department of Defence headquarters in Washington DC, killing about 300 individuals including 24 Japanese nationals and wounding many, leading to the arrest of senior Al Qaeda members. Some of the perpetrators had been residing in the United

States for over a year amongst the ordinary public.

(ii) On 22 December 2001, a British national was apprehended on board an American Airlines flight (197 passengers and crew) from Paris to Miami, found in an attempt to detonate a bomb set inside a shoe. He was a convert to Islam born in London to a British mother and a Jamaican father, and had attended a London mosque in after converting. It was found that suspected perpetrators of the September 11th attacks had been attending the same mosque.

(iii) On 12 October 2002, simultaneous multiple terrorist attacks happened at a bar and disco in Bali, Indonesia, killing 202 including 2 Japanese nationals, and wounding more than 300, including 14 Japanese. Jemaah Islamiyah members were arrested and 11 more were searched for as named suspects. Those who were arrested made statements such as: "I assisted in the manufacturing of bombs in order to kill as many Americans as possible".

(iv) On 12 May 2003, successive explosive terrorist attacks were carried out at 3 foreign compounds in Riyadh, Saudi Arabia by 15 perpetrators with automobile explosives, killing 34 including the perpetrators and wounding 194 including 3 Japanese nationals. The Saudi authorities had just exposed an Al-Qaeda arsenal, seized large amounts of weaponry and issued warrants for 19 suspects including perpetrators of the terrorist plot, 3 of which died implementing the attack.

(v) On 20 November 2003, successive explosive terrorist attacks occurred at the British Consulate General and British bank HSBC in Istanbul, Turkey, in the form of suicide bombings that involved setting explosives in the bed of a truck, killing 30 including the British Consulate General and wounding about 450, with Al Qaeda and like organisations issuing a statement to the effect that they were jointly responsible.

(iv) On 11 March 2004, 10 dynamite explosions happened

almost simultaneously in a terrorist attack on a commuter train in Madrid, Spain, killing 191 and wounding about 1900, the victims belonging to 14 different nationalities. 3 organisations issued statements to the effect of "this is in retaliation for your actions in Iraq and Afghanistan" etc., and 7 detonation devices as well as a tape of verses from the Qur'an recorded in Arabic were seized from the van thought to have been used by the perpetrators.

(iiv) On 9 September 2004, an automobile bomb attempted to drive into the Australian Embassy in Jakarta, Indonesia, killing 12 including 1 perpetrator, and wounding more than 180. The same day, an Arabic statement in the name of the East Asian Jemaah Islamiyah was posted on an Islamic website: "Australia joined the invading forces in the war in Iraq. This attack is retaliation against Australia, which is the greatest enemy of God and Islam," etc. It referred to the attack and demanded the withdrawal of Australian forces from Iraq, to the effect of: "More harm will be inflicted if the demand is not met. The automobile bombs will never cease".

(viii) On 7 July 2005, simultaneous multiple terrorist attacks (hereinafter referred to as the '**UK Simultaneous Multiple Terrorist Attacks**') were carried out in 3 locations on the Underground in central London and a moving bus, by 4 suicide bombers of British nationality with handmade explosives stuffed in backpacks, killing 56 including the perpetrators and wounding about 700. Al Qaeda etc. issued statements, and a British account indicated that 2 of the perpetrators had possibly been in contact with Al Qaeda, and that the motive for the attack was hostility against unfair treatment toward typical Muslims. The threat of homegrown terrorists and the necessity of understanding British nationals radicalized to the point of carrying out a suicide bombing were cited as lessons to be learned from the incident. 'Homegrown terrorist' refers to an individual who had led an ordinary

life in a non-Muslim developed nation but radicalizes by one influence or another, and engages in an act of international terrorism in their country of residence or aimed at interests of a country targeted by radical Islamists, and is recently the focus of attention in many countries due to incidents such as this one.

⑨ On 1 October 2005, successive terrorist attacks occurred at 3 restaurants in busy downtown etc. areas full of Western and other tourists in Bali, Indonesia, killing 23 including 3 perpetrators and 1 Japanese national, and wounding 146.

⑩ On 11 July 2006, a series of multiple terrorist attacks were carried out by setting bombs on 7 crowded trains during rush hour in Mumbai, India, killing 186 and wounding 890. The Mumbai police announced that the Islamic terrorist organisation Lashkar-e Taiba, with the assistance of the Students Islamic Movement of India, was responsible.

In addition to the above, terrorist attacks using explosives have been carried out by radical Islamists in Argentina, the Philippines, Russia, Morocco etc. Incidents of terrorist attacks using nuclear, biological and chemical substances (NBC terrorism) have taken place as well: in 2001, anthrax attacks happened in the United States; in 2002, an American member of Al Qaeda was found to have been plotting an attack on the United States using a 'dirty bomb' that spreads radioactive substances; in 2003, a radical Islamist group in London was found to have possessed substances related to the highly virulent ricin; and in February 2004, ricin was discovered in a Senate Office Building in Washington DC (Exhibits B-10, (1) and (2) of B-14, B-15, B-34-36, (1) and (2) of B-37, (1) and (2) of B-41).

iii. Japan is an ally of the United States, and carries many US related facilities that radical Islamists have made terrorist

targets. (i) On 6 May 2004, Osama bin Laden's audio statement on an Islamic website said, "The US military has promised handsome rewards to those who kill *Mujahedeen*. We too, offer the following return to those who kill Americans, allies, UN staff etc.", and "500 grams of gold (roughly 700,000 yen) for allies like Japan and Italy"; (ii) On 1 October of the same year, an audio statement of (Al-Qaeda leader) Zawahiri on Al Jazeera said, "We must not silently wait to be invaded by military forces of the US, UK etc. We should wage resistance right away. The interests of the US, UK, Australia, France, Poland, Norway, Korea and Japan are everywhere. These countries are involved in the occupation of Afghanistan, Iraq and Chechnya, and support the existence of Israel'; (iii) On 22 April 2008, Zawahiri's video statement on a Islamic website answered a question from the Associated Press on whether Japan is still an Al-Qaeda target in the following terms: "Japan insists it is cooperating with the West in their activities in Iraq, but are they not also participating in the military crusade against Muslims", and "Japan has become an ally of the US, which has occupied and plundered our land; and which has attacked Japan with conventional and nuclear weapons" (Exhibits B-16, 36 and 39).

Furthermore, in December 2003, the French national Lionel Dumont, an internationally wanted senior member of an Al-Qaeda related organisation, was arrested in Germany, which led to the revelation that he had illegally entered Japan with a counterfeit passport in July 2002 and was hiding in Niigata City. During his stay in Japan, he was known as a serious Frenchman who worked steadily and silently, but suspicions had arisen that he was fulfilling the role of an intermediary linking terrorist organisations in Europe and Southeast Asia, keeping in frequent touch with members of Islamic terrorist organisations headquartered in the UK and France, and

visiting Malaysia, where there is a branch of the radical Islamist group Jemaah Islamiyah. It became clear that another member of a radical Islamic organisation had been temporarily staying in Japan by residing with Dumont, as well as the fact that he was a devout Muslim, never failing to pray five times a day and frequenting mosques at Niigata East Port and Isesaki city in Gunma prefecture. It was found that the account he opened under a false name at the Japan Post Bank had received a few dozen transfers of several thousand to one million yen, and he is suspected to have been raising finances for terrorism and procuring supporters during his time in Japan (Exhibits B-36, C-9).

What is more, in March 2007, it was confirmed that Khalid Sheikh Mohammed, a senior Al Qaeda official in US custody, made a statement that he had been involved in plots, among others, to destroy the American Embassy in Japan. He made a statement to the effect that he had pledged allegiance etc. to Osama bin Laden in order to carry out a Jihad, and served as operations commander to plot, prepare and execute the September 11th attacks, as well as military commander for worldwide operations, directly undertaking the administration and direction of the biological weaponry manufacturing department and management of the 'dirty bomb' operations in the US (Exhibit B-19, (1) and (2) of B-37).

iv. Not only do mosques have a religious function of providing for confessions and prayers at the core of Islamic religious activities, but they are also a place for teachings— of instruction on the meaning of the Qur'an, the central religious text, and the *Hadith*— as well as a space of social interaction for Muslims to relax, eat, discourse and enforce communal bonds (from the pleadings in their entirety).

At the same time, the existence of 'home-grown terrorists' has recently caught the attention of many countries as found above in ii (viii), indicating that exposure to radical

ideas and recruitment etc. from radical Islamic groups in prisons or religious institutions possibly contribute to the process of radicalisation. In reality, the perpetrators of the UK Simultaneous Multiple Terrorist Attacks became close to each other through youth activities at mosques etc., and although the crucial factor in their radicalisation is unclear, the possibility has been indicated that they attended lectures, watched videos, and had the opportunity to read literature on radical ideas at local mosques etc. In addition, from 2 June 2006 to the 3rd of that month, the Canadian police arrested 17 individuals and seized 3 tonnes of ammonium nitrate related to, among others, suspected terrorist plots targeting the Canadian Security Intelligence Service headquarters, Canadian Association of Broadcasters, bases of the Canadian Forces, the Toronto Stock Exchange, and the Canadian Federal Parliament Building etc., and including the assassination of the Canadian prime minister. Of the suspects etc., who were all male Canadian residents, six attended the same mosque, engaging in prayers, sporting activities and discussions on Islam with an individual who held a leadership role at said mosque (the eldest of the suspect group), expressing dissatisfaction at the deployment of the Canadian Forces to Afghanistan, and receiving sermons on radical content, which point to the possibility that these were factors in their radicalisation, and the other three had reportedly been attending the same mosque as an Al Qaeda financial supporter in the 1990s (Exhibit C-10 (1)).

It has also been discovered that radical Muslim leaders have engaged in recruitment efforts for suicide bombers at London mosques (Exhibit C-10 (2)).

d) According to the facts found above in (c), numerous cases of international terrorism had occurred before around 1 January 2008, when the Information Gathering Activities took place, and the substance of the cases demonstrate that foreign terrorist organisations designated by the US government, particularly radical Islamist groups, are responsible for a high percentage of

them. As for the tactics, explosives and chemical substances etc. are used to affect an extremely large number of ordinary citizens regardless of nationality, with fatalities and the wounded reaching up to several hundred to the thousands per incident. In terms of their backgrounds, it can be said that factors such as retaliation for the Iraq War etc. or hostility toward the unfair treatment of Muslims have played a part. Moreover, these incidents of international terrorism have taken place in various regions and countries, extending to Southeast Asia, which is geographically close to Japan.

Further, Japan has been identified by multiple leaders of radical Islamic organisations as a target that is a US ally, participant in the occupation of Iraq etc., and supporter of the existence of the Israeli state. Given the revelation that a senior member of a radical Islamic organisation had been staying in the country without authorisation, and the statement by a senior member of a radical Islamic organisation to the effect that he was involved in a plot to destroy the American Embassy in Japan etc., it can be said that there had been a sufficient danger of an act of international terrorism being carried out in Japan by radical Islamist groups, with even the possibility of several hundred to thousands of civilian deaths.

Even more, considering that the terrorist incidents found in above (c) ii had all been carried out with the involvement of multiple individuals, preparing explosives etc. in advance, and targeting crowded areas with simultaneous or successive blasts, and particularly that several of the September 11th attackers had been residing in the US for over a year amongst the general public until execution of the terrorist plot, it is clear that these attacks were put into action by multiple terrorists, covertly and with a substantial preparatory period, deliberately concealing themselves within society, and pretending to lead ordinary everyday lives, all the while plotting their operation secretly and meticulously. Yet the reality is that terrorist incidents are frequently occurring around the world. Adding to this the fact that recently, there are indications of 'home-grown terrorists' undergoing transformation through contact with radical groups over the Internet or at prisons and religious institutions (above (c) ii(viii), iv), it should be said that it is not an easy task to prevent in advance acts of international terrorism by obtaining information about terrorist incidents before the fact, or detecting terrorists hiding amongst the general public.

Finally, as in the above (iv), for Muslims mosques have a significance not

only in a religious sense but also as a space for communal interaction, and there are indications that recruitment etc. by radical Muslims at religious institutions is one of the possibilities contributing to the process of radicalisation, and in reality, it is suggested that the perpetrators of terrorist incidents in the UK and Canada were recruited while attending mosques. Therefore, the early detection, for the prevention of international terrorism, of terrorists under the guise of ordinary citizens, necessitates an assessment of how Muslims constitute and run their communities. And it follows that there is no other way to discern whether one is a peaceful Muslim or a terrorist belonging to a radical Islamic group other than to make presumptions from various circumstances observable from external manifestations such as their participation, if any, in religious ceremonies or educational activities, and the position they hold in the religious community, which requires the monitoring— continuously to a certain degree— of the state of their activities, through approaching or in some cases entering mosques.

v. Thus, given the real risks of international terrorist attacks taking place in Japan, the seriousness of the damage once such an act of international terrorism happens, and the complications in early detection and prevention due to its covert nature, assessing the current circumstances of mosque attendees through the Mosque Monitoring Activities and other Information Gathering Activities should be regarded as necessary activities for the police, whose duty is to maintain public safety and order, including the deterrence of crime, to prevent the occurrence of international terrorism.

Lastly, adding to this a consideration of the courses that past incidents of international terrorism have taken, the fact that the Information Gathering Activities primarily target Muslims and that the collected information encompass matters with a religious aspect, namely, comings and goings at mosques, does not take issue with the content of followers' religious faith in Islam in and out of itself, but is instead due to the objective of preventing harm to the general public by detecting and guarding

against international terrorism by radical Muslims, by directing attention to the historic realities such as that radical Islamists, an extremely small subset of Muslims, have perpetrated acts of international terrorism, and that recruitment etc. has been conducted at religious institutions by radical Islamic groups, and not with the intention of meddling in the spiritual and religious aspects of Muslims.

The Mosque Monitoring Activities, as elaborated above, merely recorded external acts— the plaintiffs' comings and goings at mosques— through personal visits by agents, and as explained in above (1)C, there were no acts amounting to coercion regarding the said records, and moreover, effects on the freedom of religion, if any, did nothing more than invite a sense of repulsion toward the presence of police officers in and around the mosques.

To summarise, the Information Gathering Activities, even if they partially affected some of the plaintiffs' religious activities, were necessary and inevitable measures for the prevention of international terrorism, and did not violate Article 20 of the Constitution or its derivative, Article 84 of the Religious Corporations Act.

(3) On whether the Information Gathering Activities violate Article 14 of the Constitution

A) The plaintiffs allege that the Information Gathering Activities target Muslims by exclusively directing attention to their religious affiliation, and thereby constitute discrimination based on "creed" that is prohibited by the second sentence in Article 14 Clause 1 of the Constitution.

a) To be sure, of the Data, the document titled "Outline for Reinforcing Reality Assessments" (1 of Exhibit A-1) states that "Muslims with nationalities of the Organisation of Islamic Conference (OIC) countries and others" are "Targets of Reality Assessments", and accordingly, it can be held that the police, at least at the preliminary stage, determined subjects of the reality assessment by directing attention to whether or not they were Muslims. Therefore, the fact that they had made a distinction in treatment by focusing on faith on this point cannot itself be denied.

Further, as Article 14(1) of the Constitution is interpreted as prohibiting

discriminatory treatment unless there are reasonable grounds corresponding to the nature of the matter (Supreme Court 27 May 1964 Grand Bench, *Civil Cases in the Supreme Court*, Volume 18, Issue 4, Page 676 ; Supreme Court 4 April 1973 Grand Bench, *Criminal Cases in the Supreme Court*, Vol. 27, Issue 3, Page 265 *et alibi*.) As the second sentence explicitly disallows discrimination by reason of "creed", and in view of the importance of religious freedom as one of the spiritual freedoms guaranteed by the Constitution, it is necessary to examine closely whether or not there is reasonable cause for separate treatment on the basis of religion.

b) Upon analysis, (i)the Information Gathering Activities primarily targeted Muslims and collected information touching on the comings and goings at mosques, a matter with a religious aspect, not by taking issue with Muslims' faith itself, but instead by directing attention to the historic realities of international terrorism, and with the intention of preventing harm to the general public by detecting and guarding against international terrorism by radical Muslims, as opposed to meddling in the spiritual and religious aspects of Muslims; (ii)assessing the plaintiffs' religious activities etc. including circumstances of their mosque attendance through the Information Gathering Activities was a necessary activity for the prevention of international terrorism belonging within police duties; and (iii)what effect this had upon religious liberties of the plaintiffs, if any, remained within the realm of repulsion against the presence of police officers in and around the mosques, as elaborated in the above (2)B(e).

c) It then follows that even considering that distinctions were made in this case based on creed as explicitly listed in the second sentence of Article 14(1) of the Constitution, and the weight that freedom of religion carries as one of the freedoms of spirit, the different treatment had reasonable cause, and did not violate the clause in question.

B) The plaintiffs allege that despite Article 14 of the Constitution guaranteeing the right not to be discriminated against, and the State owing a duty not to promote discrimination when engaging in conduct with the effect of promoting discrimination, the Information Gathering Activities were based on prejudice that Muslims are terrorists or have a high possibility of being one, and amounted to the State conveying a discriminatory message, thereby having the effect of promoting discrimination against Muslims, and violating the plaintiffs' right not to be discriminated against.

However, as the distinctive treatment in the Information Gathering Activities has reasonable grounds as explained in above A, and as it is clear from the format etc. that the information collected by the said activities was not expected to be disclosed to the outside world, it cannot be said that the Information Gathering Activities in themselves give off a discriminatory message on part of the State.

On this point, the plaintiffs allege that even if it remains information collected and stored by the police, the danger of leaks is omnipresent, and once a leak does take place, it sends a strong message to the public that the police treat Muslims in a discriminatory matter. Yet this points back to the illegality of allowing the leak, and cannot form a basis for the unconstitutionality or illegality of the Information Gathering Activities as strictly construed.

Further, the plaintiffs allege that in light of Articles 13 and 14 of the Constitution, the plaintiffs have a legal interest in not being treated in a discriminatory manner by the State, which was violated by the Information Gathering Activities, but this line of argument cannot be accepted in light of the above explanations.

Therefore, the plaintiffs' above arguments cannot be accepted.

(4) On whether or not the Information Gathering Activities violate the freedom of not having information regarding the content or activities of one's faith collected and managed by government institutions without just reason (Article 13 of the Constitution)

A)

a) That some plaintiffs had their access to mosques or participation, if any, in religious ceremonies and educational activities noted in their Résumé-like Pages, or their missionary passion specifically noted in the "Suspicions" section of the Identification and Suspicions Pages, were found in above (1)B. Not only do these entries suggest that they are Muslims; they go further by indicating the strength of their convictions. Whatever thoughts or beliefs that a person holds are matters that directly affect an individual's interior world and personal autonomy, and is a type of information that is ordinarily unexpected to be disclosed without consent in social life.

b) However, that the prior prevention of international terrorism necessitates assessment of the realities surrounding mosque attendees, and the fact that this can only be achieved in the form of continuous assessment, to a certain degree, of their activities through a presence not only around but at times inside mosques, was explained in above (2)B(d) and (e). Furthermore, as suspicions have arisen that Lionel Dumont, who was arrested in Germany in December 2003, had been obtaining financing for terrorist acts and

engaging in the procurement of supporters while taking cover in Japan under a counterfeit passport as recognised in above (2)B(c), and as the United Nations adopted an international treaty in 1999 regarding the prevention of financial assistance for terrorism, and in light of facts such as that on 22 October 2004, the FATF (Financial Action Task Force on Money Laundering) delivered a special recommendation regarding terrorist financing, providing a nine-point fundamental framework for the detection, prevention and deterrence of terrorism and financial provisions thereof, upon the understanding that actions against financial supplies for terrorism are crucially important ((1) and (2) of Exhibit B-8), it can be said that surveying mosque attendees for terrorist supporters, such as funders of terrorism, is an information-gathering activity necessary for the prevention of international terrorism incidents. If so, it ought to be said that the police, who are under the obligation of maintaining public safety and order under Article 2 (1) of the Police Act, are required to probe and analyse the current state of social affairs, including religious activities, for each person accessing mosques, as a part of information-gathering attempts for the prevention of international terrorism.

At the same time, the Mosque Monitoring Activities took the form of agents themselves going to mosques and observing external conduct readily recognisable from the outside, such as the plaintiffs' comings and goings at mosques and circumstances of their participation in religious ceremonies and educational activities. In this sense, it cannot be said that the plaintiffs' behaviour thus assessed was not at all expected to be recognised by a third party, and even considered in the totality of the Information Gathering Activities, these did not demand the plaintiffs to prove their faith, nor did it impose prejudicial treatment or any coercion, impediments or restrictions in religious terms, their possible effects confined to the plaintiffs' sentiments of repulsion triggered by police presence around or inside mosques.

On this point, the plaintiffs allege that plaintiffs 5 and 16 were subjected to illegal searches and seizures that deviate from and abuse the rules of criminal procedure, in relation to a case with a third party suspect. Indeed, according to the facts (11(4) and 1(4) of Exhibit A-1), it can be found that searches and seizures of mobile phones etc. were conducted against plaintiffs 5 and 16. However, there is insufficient proof that these searches and seizures were illegal, so the plaintiffs' arguments cannot therefore be

accepted.

Additionally, in light of the gravity of the damage once an incident of international terrorism occurs, even considering that the plaintiffs' information gathered through the Information Gathering Activities would not ordinarily be expected to be disclosed without their consent in social life, it should be said that the Information Gathering Activities were necessary and inevitable from the point of view of preventing international terrorism.

c) Therefore, the plaintiffs' submission that the Information Gathering Activities violated Article 13 of the Constitution cannot be accepted.

B) The plaintiffs further allege that the Data contains information of the plaintiffs' nationalities, domicile, criminal history etc., which can be grounds for social discrimination, and thus amounting to sensitive information. Accordingly, they can be understood to be arguing to the effect that the collection of information other than those relating to the substance and activities of their faith also violate the freedom of not having their personal information collected and managed without reason. It can certainly be said that these information amount to the plaintiffs' privacy, with criminal history particularly relevant to a person's honor and reputation.

However, in light of the fact that there is sufficient danger of international terrorism happening in Japan, and the difficulties in its prevention through obtaining information regarding terrorist plots, or detecting terrorists concealing themselves amongst the general public, the Information Gathering Activities are necessary to prevent the occurrence of international terrorist attacks in advance and requires the compilation of various information, as explained above in (2)B. Consequently, even if the plaintiffs had not only information of the substance and activities of their faith but also information regarding their privacy including criminal records etc. collected through the process of the said activities, such constraints are inevitable in light of the above nature etc. of the Information Gathering Activities. What is more, as for the manner of the profiling, it can be conjectured, as elaborated in above (1)C, that the information was collected through cooperation with related agencies or police contact and searches etc. on the plaintiffs, which cannot be called illegal or particularly inappropriate. Hence, the Information Gathering Activities cannot be said to violate Article 13 of the Constitution.

(5) On whether the retention of personal information by the Metropolitan Police Department and

the National Police Agency violate Article 13 of the Constitution

A) The plaintiffs allege to the effect that the retention of the plaintiffs' personal information, by entry into the police database, itself violates the right not to have information related to an individual disclosed or released to a third party unreasonably, as guaranteed by Article 13 of the Constitution.

However, information-gathering activities are conducted in order to store and analyse the information thus obtained, and it has been previously established that the Information Gathering Activities do not violate Articles 13 and 20 of the Constitution. Because it naturally follows that the police may keep and use for analysis etc., information obtained through legal activities, the possession of said information does not violate Article 13 of the Constitution.

B) On this point, the plaintiffs allege, among other things, the existence of a specific danger of disclosure or release of personal information to third parties in the event of flaws in the system technology or legal regime of an information management mechanism, citing a 2008 Supreme Court case, and points out that this very case came to light by such a leak, in other words, as a result of the risk of information being readily leaked actually materialising.

However, this allegation merely argues the illegality not of the police's possession of the plaintiffs' personal information in itself, but the fact that the information was disclosed or released to third parties: namely, the occurrence of the Incident. Moreover, although the 2008 Supreme Court case, in considering whether or not the Basic Residential Registers Network System violated the freedom of not having information relating to an individual disclosed or released to third parties unreasonably, assessed, *inter alia*, the specific dangers, if any, of information leaks due to breaches etc. in the mechanics of the System, this derived from the fact that the substance of the claim in said suit focused on a deletion of the resident's card code based on the removal of an impediment against the right to personhood, distinguishable from the present case regarding a claim for State compensation on the premise that a leak has actually happened, and therefore it cannot be appropriately applied to this case.

C) Therefore, the plaintiffs' argument cannot be accepted.

(6) On whether or not there is a violation of the due process principle

The plaintiffs argue that the continuous, systematic, comprehensive, and large-scale collection, storage and use of personal information as in the Information Gathering Activities require a law that explicitly states specific objectives and standards to be met, and that Article 2 (1) of the Police Act does not serve as such a basis.

However, in light of the fact that Article 2 (1) of the Police Act designates the "prevention of crime" and "otherwise maintaining public safety and order" as police duties, the various police activities these necessitate should generally be tolerated as long as they are voluntary measures without compulsion, and it has already been established that the Information Gathering Activities are necessary activities in light of the above duties.

When the information to be collected relate to matters that risk interference with people's rights and freedoms, activities for the collection of such information should not be permitted unconditionally. However, the Information Gathering Activities are necessary and inevitable from the viewpoint of preventing international terrorism, as also previously explained.

Therefore, the plaintiffs' above argument cannot be accepted.

(7) On whether or not the gathering, retention and usage of the Personal Data violate the Act on the Protection of Personal Information

(translation omitted)

(8) On whether or not the gathering, retention and usage of the Personal Data violate the Local Ordinance on the Protection of Personal Information

(translation omitted)

(9) Summary

Consequently, as no part of the collection, storage or use of personal information by the Metropolitan Police Department and the National Police Agency can be found unconstitutional or illegal, no illegality can be found for the purposes of the State Compensation Act.

2. On Issue 2

(1) Illegality, for the purposes of the State Compensation Act, of the defendant Tokyo metropolitan government's conduct regarding the Incident

A) Firstly, although each of the reports made by the National Police Agency and the Metropolitan Police Department in December 2010 noted that the Data includes information with a high probability that they were handled by members of the police, it was not revealed specifically how the Data was removed to the outside. Police investigation into the course of the posting of the Data continued further, but the details have still not been made clear to this day, as in (4) of the Undisputed Facts.

To be sure, each of the documents that were the bases of the Data had been in the possession of the Third Foreign Affairs Division, as found in 1(1)A above. Also, as a result of wide-scope and intensive investigations conducted in an effort to solve the case, each of the reports mentioned earlier (Exhibits A-2, A-3) take note of revelations e.g. that some of the computers used in the Third Foreign Affairs

Division lacked sufficient controls, including that of the history of external memory media usage, and that the fact that removal of the information using external memory media was possible cannot be denied. This description assumes that the Data was removed from the computers used in the Third Foreign Affairs Division using external memory media, without any mention of other possibilities such as hacks by outsiders, and there is no particular evidence suggesting such alternative scenarios.

In light of this, it is fair to regard the Data as having been removed using an external memory media by a member of the police (most likely a Metropolitan Police Department employee, considering the fact that according to Exhibit A-5, access to the exclusive folder that the Data was saved in was limited to the direct administrator and senior officers).

B)

a) Then, in considering the negligence of the Metropolitan Police Department in the Incident originating from such an act of removal, as the most newly created data in the Data is dated 1 January 2009 (Exhibits A-2, A-3), the Data can be regarded as having been removed to the outside world on or after the same month at the earliest, and, according to evidence (Exhibit A-23) and the totality of the pleadings, by this time, incidents of leaks from government agencies, including the police, had been happening frequently, including incidents involving the removal of data using external memory media, incidents involving the use of personal computers, incidents resulting in the posting of police information on the Internet, and incidents causing damage in the form of the disclosure of personal information as a result of leaks, as seen in Appendix1, and it can be found that these leak cases had been reported in newspapers etc. Also, it is in the public knowledge that around that time, Winny was causing numerous leaks onto the Internet from computers other than that of the police and government agencies.

Further, the Data contained Personal Data which is the plaintiffs' personal information, and particularly, the content included matters that directly relate to the inner world of individuals and the autonomy of personhood, in the form of information that not only directly revealed that the plaintiffs are Muslims but also indicated the strength of their faith, as well as criminal history, which directly relate to a person's honour and reputation, as previously found and explained. It can be said that such information, even

among the contents of personal privacy, amounts to information that one least wants others to know, and such information, once leaked onto the Internet, carries a risk of being communicated to the general public due to their high capacity to diffuse and spread, and it is extremely difficult, if not almost impossible, to later retrieve all of the information.

As a result, it can be said that it was sufficiently foreseeable to the Superintendent General that if the Data were removed and connected to an external computer, there was a danger of it being leaked onto the Internet through Winny etc., being communicated to the general public, and inflicting great damage to the plaintiffs.

Accordingly, the Superintendent General was under a duty of care in the area of information control to take thorough anti-leak measures so that the plaintiffs' personal information would never be leaked.

b) In response to this, the defendant Tokyo metropolitan government, citing a 1986 Supreme Court case, argues to the effect that clearly it cannot be said that the specific course of events leading to the Leak Incident, much less the outcome, namely, of the Data being posted on the Internet, was foreseeable to the Superintendent General, in light of the circumstances such as (i) Administrative Notices (On the Administration of Rules Regarding the MPD Information Security) prohibiting employees from removing electromagnetic memory media that constitute the police information system from the police buildings; (ii) the illegality of data removal, subject to criminal and disciplinary penalties as a violation of Article 34 of the Local Government Employee Act; (iii) the multiple acts required in the course of posting the Data on the Internet; and (iv) the complete absence of information leak cases through the removal of data after the February 2008 completion of the introduction of an automatic encryption system when recording data on external memory media from terminal devices (hereinafter referred to as the Automatic Encryption System).

However, penalty rules and administrative notices themselves do not make the removal of data impossible or difficult in a physical or technical sense, and as previously noted, there had already been numerous occasions of leaks from computers onto the Internet through Winny, by around January 2009. As for the Automatic Encryption System, there is insufficient evidence to hold that it had been installed on every computer used in the Third Foreign Affairs Division during the period between that month and

the October 2010 date of the Incident. In fact, evidence (Exhibit A-5) shows that some computers used in the Third Foreign Affairs Division lacked the Automatic Encryption System. Accordingly, none of the points raised by the defendant Tokyo metropolitan government can be said to defeat the Superintendent General's foreseeability illustrated above in subparagraph (b).

The defendant Tokyo metropolitan government also cites in its argument a 2005 Sapporo High Court case ((1) of Exhibit C-11) denying the foreseeability for the manager etc. in an information leak case, but this judgment can be distinguished from the present case due to the specific facts giving rise to foreseeability at the time of the incident. Therefore, consideration of this case does not influence the above decision.

C) Next to consider is whether or not the Superintendent General breached his duty of care in information management.

a) Evidence (Exhibits A-2, A-3, C-6, C-7) show that the Metropolitan Police Department established and published the "Rules Regarding Information Security of the MPD" (hereinafter referred to as the Security Rules) etc. on 28 June 2005. This (i) appointed a Metropolitan Police Department Information Security General Officer (hereinafter referred simply as the 'General Officer') to the Metropolitan Police Department headquarters, imposed with a duty to make efforts to appropriately maintain and manage computers, terminal devices, electronic communication lines or any connected machines, and electromagnetic memory media etc. (Article 10 of the Security Rules). Specifically, only authorised electromagnetic memory media could be used in police duties, in order to secure regular functioning of the police information system etc. and to prevent information leaks; Information Management Officers (whose duty involves information security relating to the police information system etc. in order to maintain the information security within their division) who accept into their division an electromagnetic memory media for the use of police duties were to receive an inspection by the head of their division at least once a month regarding its management; and Information Managers (whose duty involves the management of computers etc. in order to maintain information security relating to the police information system etc. within their post), if delivered an electromagnetic memory media by the Information Managing Officer, were to store it in a secure locker etc.; the handling of electromagnetic

memory media was to be disclosed in a "Electromagnetic Memory Media Removal and Return Log" (7 (5) of the Administrative Notice No. 2 etc.). It also (ii) imposed an obligation on the General Manager to encrypt necessary information according to the objectives of the duty, in order to maintain information security (Article 11 of the Security Rules). Specifically, when storing information on an electromagnetic memory media, encryption measures were to be taken unless authorised by the General Manager, and the Information Manager was to verify trails of exports onto the electromagnetic memory media by the encryption file, and report the results to the head of the division (8(1) and (4) of the Administrative Notice No. 2). It further (iii) imposed an obligation on employees to properly handle the police information system etc. as well as the information processed by it (Article 14 of the Security Rules), specifically, prohibiting in general: transferring electromagnetic memory media to others, computers relating to personal ownership, bringing electromagnetic memory media etc. into the National Police Agency building, and removing devices and electromagnetic memory media comprising the police information system etc. from the National Police Agency building (11(3), (10), and (11) of the Administrative Notice No. 2).

b) However, none of these measures made the removal of data from the building inherently impossible or difficult in a physical or technical sense, and it can be said that compliance with the above rules ultimately depended on the actions of each individual employee. What is more, in terms of the above (a)(i) and (ii), no evidence clarifies to what degree each of the procedures such as inspection of the management of electromagnetic memory media by the head of the division, entry into the "Electromagnetic Memory Media Removal and Return Log" of the removal and return of electromagnetic memory media, and the verification and reporting of trails of exports to electromagnetic memory media by encryption files, were practiced in reality.

As for the Automatic Encryption System, the fact that computers lacking its installment were being used at the Third Foreign Affairs Division was found above in B(b).

If so, as merely establishing and publishing security rules etc. and introducing an automatic encryption system does not ultimately serve as a conclusive factor in preventing information leaks to the outside, it should be

said that constructing a management regime to ensure actual compliance of the Security Rules etc. by each employee or information manager etc. was necessary and essential as a genuine preventative measure.

c) Yet it has been revealed that the management of trails of the history of external memory media usage etc. for some of the computers used in the Third Foreign Affairs Division was insufficient as held above in (a), and thus it must be observed that the management regime to ensure the actual compliance of security rules etc. in the Third Foreign Affairs Division was inadequate, and that this fact led to the removal of data using external memory media.

It must therefore be said that the Superintendent General negligently breached his duty of care in information management, which is illegal for the purposes of the State Compensation Act. As such, it follows that the defendant Tokyo metropolitan government is liable.

(2) Illegality, for the purposes of the State Compensation Act, of the defendant Japanese government's conduct regarding the Incident

A) The plaintiffs allege to the effect that under Article 7 (1) of the Security Orders, The National Police Agency must designate an Inspection Officer to perform inspections relating to the police information system, and in light of duties that the role entails, as established by Article 7 (3), the Inspection Officer was under a duty of care, through opportunities such as regular inspections, to accurately assess the substance of the numerous information leak incidents between 2006 and 2008, analyse their causes and responses, reflect them in the Annual Information Security Inspection Plan, and secure, by the 2009 regular inspection of the Metropolitan Police Department at the latest, the implementation of measures to prevent information leaks using external memory media, and that breach of this duty resulted in the Incident.

B) Upon consideration, it is true that the National Police Agency, under Article 7(1) of the Security Orders (Exhibit B-28), is to appoint an Inspection Officer to supervise the execution of inspections regarding information security related to the police information system, and according to the Execution Guidelines for Police Information Security Inspections (Exhibit B-30), the Inspection Officer, in conducting regular inspections of the prefectural police etc., is to formulate an Annual Information Security Inspection Plan, and based on this, establish an Inspection Execution Plan for each individual inspection; and after conclusion of the regular inspection, the Inspection Officer is to create an Inspection Report and

submit it to the Chief Information Security Manager, who, based on the Report, instructs the heads of the divisions in question on necessary matters such as improvements to be made; the leaders receiving said instructions are to promptly take adequate measures based on the substance of the instructions, and report back to the Chief Information Security Manager on the outcome; and in addition, the Inspection Officer is to execute Special Inspections when the necessity of such is particularly recognised by the Chief Information Security Manager. The fact that the Incident was due to a breach of the duty of care in information management in the Third Foreign Affairs Division has already been elaborated on, and the possibility that the Incident might have been prevented had the inadequacies in information management been indicated at the National Police Agency's inspection stage, cannot itself be denied.

However, inspections carried out by the National Police Agency's Inspection Officer, besides the annual regular inspection, are special inspections responding to particular necessities, and are not of a kind involving, for instance, an Inspection Officer permanently stationed in each division to monitor compliance with information security (the National Police Agency is in a position to supervise the prefectural police in general, and it is impossible for Inspection Officers to be permanently stationed in each division of all the prefectural police forces in order to monitor compliance with information security, and it cannot be said that a duty to carry out such inspections exists), so cases in which the defendant Japanese government would be held liable for the Inspection Officer's inspections should be said to be limited to cases, for example, such as a chronic failure to inspect, or a failure to articulate an inadequacy found through an inspection, and such circumstances cannot be found regarding the Incident, in compiling the totality of the evidence in this case.

On the other hand, evidence (Exhibit B-52) shows that the 2009 Police Information Security Inspection on the Metropolitan Police Department and the prefectural police etc., was carried out with a focus on improvements in response to indications from past inspections etc., the implementation of increasingly thorough preventative measures against the reoccurrence of information leaks, the implementation of information security measures concerning external memory media etc., the management of the police information system, and measures against breaches of information security. As a result, in some divisions inappropriate circumstances were identified such as (i) indications of the use of unauthorised external memory media on computers unable to acquire trails of

their use; (ii) that encryption when recording information on external memory media was not thoroughly practiced; and (iii) verification of the trails of exporting information onto external memory media done by the very employees using the said media. Considering these findings, improvements were requested of the divisions in question to (i) reinforce the management and inspections etc. of the use of computers and external memory media; (ii) make thorough encryptions when recording information onto external memory media; (iii) have the manager of media usage verify trails in the import and export of information regarding external memory media; and to report the results to the administrative manager etc.

Further, according to evidence (Exhibit A-23) and the entirety of the pleadings, the National Police Agency implemented countermeasures for each of the following cases listed on Appendix1: (i) In response to the leak of personal information onto the Internet at A and B police agencies in March 2006: measures such as the inspection of personal computers etc.; submission of confirmation documents (that no employee was to manage police information on personal computers or external memory media that is not authorised to use on duty, or use computers running Winny (both of which are held to standards at the time)); a reinforcement of information management based on remarks made by the Chief Cabinet Secretary at the meeting of administrative vice-ministers etc. held on the 9th of the same month, to the effect that information leaks through the use of personal computers were creating an extremely concerning situation, and that the relevant ministries and agencies were to reinforce warnings to each and every employee regarding computer use against information leaks; a sweep of personal computers used on duty; reinforcement of inspections; and special inspections against all of the prefectural police agencies etc., (ii) in response to the leak of personal information onto the internet from C police agency in February 2007: measures such as compliance with fundamental measures in information security including the implementation of self-inspections and individual interviews; compliance with rules regulating the management of police information; and limiting the use of external memory media as well as taking encryption measures etc., (iii) in response to the leak of personal information onto the Internet from D police agency in June of the same year: measures such as the reinforcement of fundamental matters regarding the management of police information; deleting of unnecessary police information; sweeping unauthorised personal devices; and inspecting personal computers etc., (iv) in response to the leak of police

information onto the Internet from E police agency in May 2008: measures such as the inspection of personal computers and actual devices; prohibition on the use of unregistered external memory media; resubmission of confirmation documents; small group discussions etc. to raise awareness; recording and managing trails; and limiting the use of external memory media drives by USB keys.

Accordingly, it can be found that the National Police Agency's Inspection Officer had been carrying out the necessary regular inspections and implementing possible measures every time an information leak onto the Internet happened.

C) Therefore, the plaintiffs' above argument cannot be accepted, and the defendant Japanese government cannot be found liable for the Incident.

(3) Illegality, for the purposes of the State Compensation Act, of the defendants' omissions following the Incident

A) The plaintiffs allege to the effect that the Metropolitan Police Department is liable in state compensation because while it should have taken concrete measures such as promptly acknowledging the Data as documents created and managed by the Metropolitan Police Department and the National Police Agency, and making requests against Internet providers etc. continuing to publish and post the material to delete them, in reality the Metropolitan Police Department and the National Police Agency refused to acknowledge that they had created and managed the documents in the Data, and failed to take effective measures until admitting to the leak and making a formal apology on 24 December 2010.

B) Upon consideration, certainly, according to the pleadings in their entirety, the Metropolitan Police Department and the National Police Agency could not have comprehensively deleted the Data including the plaintiffs' personal information.

However, evidence (Exhibits A-2, A-3) show that the National Police Agency recognised the Incident on 29 October of that year, contacted the Metropolitan Police Department, and in cooperation, commenced investigations etc. At the same time, it can be found that the Metropolitan Police Department immediately requested cooperation, to delete the Data, from providers etc. that offered spaces for webpages posting them.

Also, despite the fact that completely deleting the Data, which included the plaintiffs' personal information, was not ultimately possible as above, according to the totality of the pleadings, the reason for this was a combination of multiple factors such as that in this Incident, methods were used to inhibit identification of the leak source such as transiting through numerous overseas servers; that due to

Winny, the file sharing software used, retrieval of the information was virtually impossible; and that the police could not compel erasure of the Data from the servers onto which the leaked information was posted, merely making requests against overseas servers to voluntarily delete them.

Consequently, it is fair to say that the Metropolitan Police Department and the National Police Agency, in cooperation, fulfilled their duty as they should, and cannot be said to have failed in their duty to mitigate loss as the plaintiffs claim.

While this Court notes the fact that the defendants have not acknowledged that the Data consists of documents created and managed by the police even in this lawsuit, evidence (11(1)-(114) of Exhibit A-1) and the totality of the pleadings demonstrate that the Data contains information regarding individuals or organisations, information about cooperation with foreign countries, as well as information-gathering activities by the police etc., and it can be found that a straightforward admission that the Data had been created and managed by the police involves the risk of further harming the rights and interests of those individuals and organisations, as well as damaging the trust of the countries in question and impeding the appropriate execution of information-gathering activities etc. regarding future police strategies against international terrorism. Thus, it cannot be said that this itself is an act that is independently illegal for the purposes of the State Compensation Act.

C) Therefore, the above arguments of the plaintiffs cannot be accepted.

3. On Issue 3

(1)

A) The Incident was one in which the plaintiffs' personal information was posted on the Internet. It included types of information that one least wishes to be disclosed to others, such as information on the plaintiffs' faith and prior convictions. What is more, there was also data that took the form of a page noting relationships etc. with another Muslim individual under the heading "Suspicions", and while these entries were confined to piecemeal information, it is difficult for a third party not to receive the impression that the plaintiffs are terrorists, supporters of such, or at least suspected by the police along those lines. Furthermore, once such information is leaked onto the Internet, due to their tendencies to diffuse and spread, there is the possibility that the information could extend to the entire world, and it is difficult to completely erase the information, and in reality, the Data had been downloaded onto more than 10,000 computers in more than 20

countries and regions as of 25 November 2010, less than one month since the Incident, as per (2) of the Undisputed Facts. In view of these points, it can only be said that the invasion of privacy and defamation that the Incident inflicted on the plaintiffs was of great magnitude.

Further, the plaintiffs have made testimonies such as the following: because of the leaked Data, their family may face discrimination, harm or disadvantages based on prejudice; their familial relations may be adversely affected; the mutual trust among Muslims was damaged; they were forced to become paranoid in everyday life and obsessed over people's perceptions; it became difficult to work or secure permanent employment, or their businesses came to suffer; and that they no longer have a peace of mind in returning to their home countries, when considering the possibility of being suspected as a terrorist (1-17 of Exhibit A-34). The plaintiffs' concerns are fully understandable in light of the above content and nature of the information contained in the Personal Data, and can be called characteristics of detriment from the invasion of privacy and defamation that the plaintiffs suffered.

B) On the other hand, it must also be considered that with the exception of economic damage to some of the plaintiffs in the form of loss of employment and revenue etc., the above detriment to the plaintiffs have not yet materialised at this point, and remain vague insecurities about matters that may or may not eventuate in the future. On this point, the plaintiffs argue to the effect that some of the plaintiffs have: suffered bankruptcy in their business because despite directing capital and efforts toward establishing a foreign branch of the company they manage, their visa was denied due to the foreign authorities receiving notice of this false information regarding investigations, and the entire plan fell through; seen a drastic decrease of revenue at the restaurant they manage; effectively been fired from the restaurant they worked at; and lost their employment at an embassy. However, such matters differ greatly depending on the individual circumstances of each plaintiff, and it should be said that it is not proper to take into consideration such individual matters in calculating the amount of reparations.

C) Incidentally, plaintiffs 1 and 4 were merely listed on others' Résumé-like Pages as spouses, as found previously.

However, although a profile photo of plaintiff 1 has not been leaked, he was listed on the "Familial Relations and Acquaintances" section of plaintiff 2's Résumé-like Pages as her husband, along with his name, date of birth, address and employer, and the "Information on Suspicions" section of plaintiff 2's

Identity and Suspicions Page noted that he holds a lecturer-like position at the mosque and is highly reputable as an Islamic lecturer, and continuously participates in workshops, special prayers and sermons etc. held at the mosque, and that they passionately engage in missionary activities as a couple, as found in the above 1(1)B(b) and (d). As details of his religious activities have been leaked, and is entered under the "Information on Suspicions" section, depending on the reading of the leaked information, plaintiff 1 could, along with plaintiff 2, be mistakenly regarded as a terrorist supporter, and it should be said that it is not proper to differentiate his level of emotional suffering in comparison to the other plaintiffs.

In contrast, as for plaintiff 4, she is merely listed as plaintiff 3's wife in the "Familial Relationships and Acquaintances" section of plaintiff 3's Résumé-like Pages, with her name, date of birth and address noted, but not her employment. Also, on plaintiff 3's Identity and Suspicions Page (29 of Exhibit A-1), she only has her name and date of birth noted as his wife, under the section of "Family" within "Identity Matters". There is no mention of plaintiff 4 in the "Information on Suspicions" section. As a result, in relation to plaintiff 4, although the extent of her emotional suffering caused by the disclosure of information depicting her spouse as if he were a terrorist cannot be dismissed, there exists a substantial difference in the quality and quantity of her leaked personal information in comparison with the other plaintiffs, and it must be said that her emotional suffering is significantly less than the others.

D) The defendant Tokyo metropolitan government has consistently declined to admit that the Data was information held by the Metropolitan Police Department, and this fact can be counted as one of the reasons why the plaintiffs were forced to go through the trouble of filing this lawsuit. Therefore, even on the premise that this in itself is not considered an independent illegality for the purposes of the State Compensation Act, it should be taken into account in calculating the reparations. The fact that revelations by the defendants on this point risks adverse effects on foreign relations is as held above in 2(3)B, but this does not justify burdening the plaintiffs in the previously stated ways.

(2) Considering these matters comprehensively, it is held that 5 million yen each for each of the plaintiffs with the exception of plaintiff 4, and 2 million yen for plaintiff 4, is fair compensation for the plaintiffs' emotional suffering caused by the defendant Tokyo metropolitan government's breach of its duty of care in information management regarding this case. Additionally, in light of the substance of this suit, advancement of their claims

through legal representation was necessary, so 10% of the reparations for each plaintiff (namely, 500,000 for each of the plaintiffs except for plaintiff 4, and 200,000 for plaintiff 4) should be held to amount to legal costs as damages within the scope of legal causation from the defendant Tokyo metropolitan government's above breach in their duty of care.

As this case is a claim for uniform reparations, this Court initially considered adopting the minimum amount corresponding to plaintiff 4's emotional suffering for all the plaintiffs, but because this would be too low for the others, separated out plaintiff 4, and as for the remaining plaintiffs, disregarded individual matters as previously stated, and translated their common detriment into a monetary amount in order to calculate a uniform sum of reparations.

4. On Issue 4

(translation omitted)

IV. Conclusion

Given the above circumstances, the plaintiffs' claim against the defendant Tokyo metropolitan government has a basis to the following limit and is thereby granted: for each plaintiff with the exception of plaintiff 4, a sum of 5.5 million yen in damages as well as money accruing therefrom at an annual interest rate of 5% during a period starting from 26 July 2011 up to a date when the payment will be completed; and for plaintiff 4, a sum of 2.2 million yen in damages as well as money accruing therefrom at an annual interest rate of 5% during a period starting from 26 July 2011 up to a date when the payment will be completed. The remainders of their claim against the defendant Tokyo metropolitan government, as well as their claim against defendant Japanese government, are dismissed for a lack of basis. Accordingly, judgment is rendered as described in the main text.

A declaration for the suspension of provisional execution will not be made, as it is not proper.