



April 4, 2013

**SENT BY EMAIL**

Secretary  
Canadian Transportation Agency  
Ottawa, ON K1A 0N8

Dear Madam Secretary:

**RE: Complaint about United Air Lines, Inc.'s prohibition against  
onboard photograph and audio or video-recording**

Please accept this letter as the answer of United Air Lines, Inc. (“**United**”) to the February 24, 2013 complaint of Dr. Gábor Lukács, in accordance with the Agency’s letter of March 14, 2012.

Lukács submits that a statement in United’s onboard Magazine, *Hemispheres* (“**Hemispheres**”), regarding onboard photography and video is contrary to section 18(b) of the *Air Transportation Regulations* (“**ATR**”) because no similar statement is found in United’s Contract of Carriage (“**Tariff**”). Lukács also submits that the statement in *Hemispheres* is unreasonable.

It is United’s position that the statement regarding onboard photography and video-recording found in *Hemispheres* is a reflection of society’s privacy expectations while travelling onboard an aircraft. It is not a term or condition of carriage or a policy that is required to be listed within United’s Tariff. Consequently, it is not a false or misleading statement with respect to the licensee’s air service or any services incidental thereto. Further, United submits that the statement regarding onboard photography and video-recording is reasonable.

**Summary of Argument**

The statement appearing in *Hemispheres* is not a term or condition of carriage. Rather, the statement reflects United’s view of what types of behavior and activities are appropriate and inappropriate on its aircraft. United does not treat the statement as a term or condition of carriage and United does not refuse carriage or remove passengers solely for acting contrary to the statement. Further, if United believed that compliance with the statement should be a term or condition of carriage it would have included the term within its Tariff. The Agency has previously recognized that subject to applicable legislation and regulations, air carriers have the



flexibility to establish their terms and conditions of carriage.<sup>1</sup> United submits that applicable legislation and regulations do not require that United treat the statement as a term or condition of carriage and that the Agency should uphold United's decision to not include the statement within its Tariff.

United also submits that the statement does not mislead passengers. The fact that the statement uses strong terms, such as "prohibit" does not mislead passengers as to the content of United's Tariff. Further, the statement does not state any consequences for non-compliance. Lastly, passengers are aware that many behaviors which may disrupt other passengers of flight crew are likely to be prohibited on an aircraft. The fact that passengers receive advanced notice in an onboard magazine that a specific type of disruptive behavior is prohibited does not mislead passengers to believe that compliance with the statement is a term or condition of carriage.

The statement in *Hemispheres* is not a term or condition of carriage and as such the Agency need not determine whether the statement is reasonable pursuant to section 111(1) of the ATR. Nevertheless, United submits the statement is reasonable. In particular, the statement reflects society's expectations regarding video-recording and photography on aircraft and balances individuals' interest in recording their flight with other passengers' privacy expectations, flight crews' privacy expectations, and the need to ensure safety and security of the aircraft. Further, there are less privacy intrusive means of addressing the concerns that Lukács raises in his complaint

### **Preliminary Issue**

Lukács states that the complaint is motivated by a media report of a passenger being removed from a United flight for taking photographs. United submits that the media report attached to the complaint and the incident as whole should be disregarded by the Agency in deciding this matter. The incident at issue did not involve an air service to or from Canada. The alleged incident therefore occurred outside of the Agency's jurisdiction and Lukács does not have standing to complain about an incident affecting another individual, particularly given that he was not present. More importantly, the media article presents only one side of the incident and it would be improper to rely on it as factual basis for deciding whether the statement in *Hemispheres* is a term or condition of carriage, misleading, or unreasonable.

### **Background on the statement in *Hemispheres***

In 2009, one or more passengers took photographs and extended video-recordings of another passenger's ordinary travel activities while travelling on a United flight without that passenger's consent or knowledge. Subsequently, the recordings were disseminated on the internet. The

---

<sup>1</sup> CTA Decision No. 613-C-A-2006 at para 49; CTA Decision No. 259-C-A-2006 at para 23; CTA Decision No. 565-C-A-2008 at para 15.



passenger whose image was recorded and disseminated complained to United that these other passengers had invaded his privacy, that such behavior was inappropriate, and that flight crew should not allow such behavior in the future. The complaining passenger inquired whether United had a policy to deal with non-consensual video-recordings and photographs on-board its aircraft. United responded that it did not, but that it would consider the matter.

United considered several factors when deciding whether or not to create an onboard privacy statement. First, passengers have a legitimate interest in documenting their travel. Taking pictures and videos of travel companions, of the view outside the window or even a meal is reasonable. Second, society is protective of individuals' privacy and the fact that an individual is on an aircraft does not mean that he or she must forego all of his or her privacy interests. Third, the unique nature of air travel, whereby individuals sit in close proximity and have little ability to remove themselves from the presence or activities of others, and the importance that society places on individuals' privacy means that non-consensual photographs and recordings of other individuals could result in an unnecessarily unpleasant experience for individuals or disorderly conduct that affects the safety and security of the flight. Fourth, flight crew also have privacy interests. The fact that an individual is an employee of United does not mean that any passenger should be able to record their every move. Further, recording and photography can distract crew, affect morale, and interfere with their duties, and hence Federal Aviation Regulations and comparable regulations in other jurisdictions including Canada. Fifth, various jurisdictions have laws—regulatory, common law, and criminal law—governing privacy, and passengers and flight crew expect other passengers to behave according to these laws. Sixth, surveillance recording of flight crew equipment and procedures could affect the safety and security of the flight or future flights. Flight crew follow various safety and security procedures and practices throughout a flight and the study of these procedures could jeopardize the safety and security of flights. United was and is particularly conscious of the 9/11 Commission Report authored by the United States National Commission on Terrorist Attacks, which found that the 9/11 terrorists engaged in multiple surveillance flights as part of their preparations.<sup>2</sup> Lastly, it is widely accepted that individuals and companies can prohibit or restrict the use of photography on private property and many businesses do so for the comfort of their customers and employees.

Balancing these factors, United drafted a policy to guide flight crew in dealing with video and audio recording on flights. In sum, individuals can record their personal events—i.e. their meal, their companions, the view from outside their window—but video-recordings of other individuals (passengers and crew) should occur only with their consent, and recordings of flight procedures, airline equipment, and the interior of the aircraft should occur only with the consent of United. The policy is not a rule, term, condition, or regulation; rather it is a guide. Depending on the circumstances of the particular case, if a flight crew member observes a passenger video-recording another passenger or crew or trying to film certain parts of the aircraft (e.g. the cockpit

---

<sup>2</sup>Appendix A: National Commission on Terrorist Attacks, The 9/11 Commission Report at 242, 243, 245, 248, available at <http://www.9-11commission.gov/report/911Report.pdf>.



while the door is open), the flight attendants will request that the individual cease their activity. Failure to cease recording is not *per se* grounds to remove a passenger and/or refuse carriage. However, if the flight crew determines that the behavior of a passenger is sufficiently disruptive to affect the safety and security of the flight—e.g. it is creating conflict with other passengers or that the recording individual has a malicious intent—United will exercise its right to remove the passenger or refuse carriage pursuant to Rule 21 of its Tariff.

After informing United employees about the policy, flight attendants suggested that a statement reflecting the policy be made easily available so that they could refer passengers to it rather than having to repeatedly explain to passengers what was appropriate and what was not. United followed this suggestion and for the last four years it has included a statement within the *Hemispheres* onboard magazine. The statement, which appears at the bottom of a page discussing the use of electronic devices while on board an aircraft, reads:<sup>3</sup>

**ONBOARD PHOTO AND VIDEO** The use of still and video cameras, film or digital, including any cellular or other devices that have this capability, is permitted only for recording of personal events. Photography or audio or video recording of other customers without their express prior consent is strictly prohibited. Also, unauthorized photograph or audio or video recording of airline personnel, aircraft equipment or procedures is always prohibited. Any photography (video or still) or voice or audio recording or transmission while on any United Airlines aircraft is strictly prohibited, except to the extent specifically permitted by United Airlines.

This statement is similar to one which appears in *American Way*, American Airlines' onboard magazine.<sup>4</sup> A copy of the American Airlines statement is attached as Appendix C.

In United's view, "personal events" include events unique to the passenger. Filming travel companions (with their consent), meals, and the view from the window are examples of "personal events". When the subject matter being recorded exceeds the "personal event" category will depend on the circumstance. A key factor will be the nature of and degree to which the recording or photograph records other passengers, crew or United equipment and procedures. For example, a video-recording of a travel companion that inadvertently records another passenger for a brief moment (e.g. as the camera moves) is unlikely to be viewed by other passengers or crew as inappropriate or unreasonable. Similarly, a recording of companions that necessarily captures the interior of the cabin immediately surrounding the passengers would be reasonable in most circumstances. However, a recording of a snoring passenger in the next seat or attempts to record the cockpit when the cockpit door opens would be inappropriate.

Lastly, flight crew members exercise their discretion in dealing with photography and video-recordings onboard aircrafts. Flight crew members have expertise and experience when it comes to managing passengers in the confines of an aircraft. In certain circumstances, it may be necessary for the flight crew to intervene as soon as inappropriate use of photography or video-

---

<sup>3</sup> Appendix B, *Hemispheres Magazine*, August 2012 at 129.

<sup>4</sup> Appendix C: *American Way* (April 1, 2013), p. 80.



recording equipment occurs. In other circumstances, it may be appropriate to allow minor transgressions.

***Issue 1: Is the statement a term, condition or policy that is must be included in United's Tariff?***

United submits that the onboard photo and video statement in *Hemispheres* is not a term or condition of carriage and need not be included within its Tariff.

***a) The meaning of "term and condition of carriage"***

Section 122(c) of the ATR provides that a Tariff must include the terms and conditions of carriage, including those pertaining to certain enumerated matters. Lukács submits that the statement is a term and condition of carriage; United submits that it is not. Thus, the Agency must determine whether the statement is a "term or condition of carriage".

"Terms and conditions" is not defined in the ATR or the *Canada Transportation Act*. Consequently, the Agency must interpret these terms, which requires that the words be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the ATR and the Act, the object of the ATR and the Act, and the intention of Parliament.<sup>5</sup> Oxford online dictionaries defines "terms" as "4 (terms) conditions under which an action may be undertaken or agreement reached; stipulated or agreed requirements".<sup>6</sup> It defines "conditions" as "3 a situation that must exist before something else is possible or permitted".<sup>7</sup> Black's Law Dictionary defines "terms" as "3 Provisions that define an agreement's scope; conditions or stipulations <terms of sale>".<sup>8</sup> Black's Law Dictionary defines "condition" to mean "1 A future and uncertain event on which the existence or extent of an obligation or liability depends; an uncertain act or event that triggers or negates a duty to render a promised performance [...] 2 A stipulation or prerequisite in a contract, will, or other instrument, constituting the essence of the instrument".<sup>9</sup>

United submits that the phrase "terms and conditions" as it appears at Section 122 of the ATR refers to stipulations, prerequisites, and requirements that must be met for a carrier to transport a passenger. It follows that a "policy" only needs to be included within the tariff if it is a stipulation, requirement or condition for carriage. The view that carriers' tariffs only need to include those stipulations and conditions that are prerequisites and requirements for carriage, rather than setting out every detail of how the airline will deal with every possible circumstance

---

<sup>5</sup> *Sun Indalex Finance, LLC v. United Steelworkers*, 2013 SCC 6 at para 136.

<sup>6</sup> Appendix D: Oxford Dictionaries, available at [www.oxforddictionaries.com](http://www.oxforddictionaries.com), "term".

<sup>7</sup> Appendix D: Oxford Dictionaries, available at [www.oxforddictionaries.com](http://www.oxforddictionaries.com), "condition".

<sup>8</sup> Appendix D: Bryan A. Garner, ed., *Black's Law Dictionary*, 8<sup>th</sup> Ed (Thomson West: St. Paul, 2004).

<sup>9</sup> Appendix D: Bryan A. Garner, ed., *Black's Law Dictionary*, 8<sup>th</sup> Ed (Thomson West: St. Paul, 2004).



is supported by the Agency's recent decision *Lukács v. Porter*.<sup>10</sup> In that case, Lukács argued that a contract of carriage must include precise departure and arrival times. The Agency rejected Lukács's arguments, stating, "It is simply impractical to write a tariff so precise that it addresses every conceivable situation".<sup>11</sup>

***b) The statement in Hemispheres is not a term or condition***

United submits that the onboard photo and video statement is not a term or condition of carriage; rather it is a statement reflecting United's view of what types of behavior and activities are appropriate and inappropriate on its aircraft and notifies passengers thereof. United does not treat the statement as a term or condition of carriage. United does not refuse carriage or remove passengers solely for acting contrary to the statement. Further, had United intended this policy to be a term or condition it would have included the term within its Tariff. The Agency has previously stated that "air carriers should have the flexibility to establish their terms and conditions of carriage and to price their services as they see fit, subject to legislative or regulatory constraints", and the Agency should uphold United's decision to not include the statement within its Tariff.<sup>12</sup> Further, United is in the best position to decide whether or not a passenger video-recording or photographing other passengers, crew or United equipment and procedures poses a sufficient threat to safety or security to warrant refusing carriage to that passenger.

Further, the fact that *Hemispheres* includes the statement does not make it a term or condition. United crew will prohibit behavior that unreasonably affects the comfort of passengers or interferes with duties of the flight crew. For example, flight attendants would most likely prohibit a passenger from playing a musical instrument mid-flight or pointing a flashlight in the faces of sleeping passengers. The fact that *Hemispheres* advises passengers in advance that video-recording other passengers without their consent is inappropriate, but does not state that playing a musical instrument is inappropriate, does not make the statement on inappropriate photography and video-recording a term or condition of carriage.

The fact that the statement uses the term "prohibited" also does not make it a term or condition. Flight crews may "prohibit" passengers from all kinds of activities and behavior such as entering business class, using business class lavatories, or playing loud music. The fact that a flight attendant may forbid or prohibit such behavior for the comfort of other passengers does not make it a term or condition of carriage.

Furthermore, the Agency must be wary of interpreting section 122 of the ATR as requiring airlines' tariffs to identify all types of behavior that the airline may view as unreasonable,

---

<sup>10</sup> CTA Decision No. 16-C-A-2013.

<sup>11</sup> CTA Decision No. 16-C-A-2013 at para 47.

<sup>12</sup> CTA Decision No. 613-C-A-2006 at para 49; CTA Decision No. 259-C-A-2006 at para 23; CTA Decision No. 565-C-A-2008 at para 15.



disruptive, unwarranted or inappropriate. Such an interpretation would result in airlines having to list an infinite number of behaviors and actions that a flight crew may, depending on the circumstances, discourage or forbid. The playing of a musical instrument is one example; indiscriminate use of a portable flashlight is another. Including a statement such as that which appears in *Hemispheres* within an onboard magazine can prevent conflicts between passengers, prevent passenger embarrassment by being confronted by flight crew, and provide reassurance to other passengers that United will take appropriate steps to ensure that other passengers do not unreasonably invade their privacy.

The burden is on Lukács to establish that the statement is a term or condition of carriage and he has failed to meet his burden. Lukács has produced no credible evidence that United applies the statement as a term or condition of carriage. The news article appended to his complaint is hearsay, presents only one side of story, and does not demonstrate that United applies the statement as a term or condition. Consequently, the Agency should give it no weight. Lukács's complaint is premised on the assumption that the statement is a term or condition of carriage. His failure to provide sufficient evidence establishing the statement as a term or condition of carriage is a material deficiency in his complaint.

For the reasons above, United submits that Lukács has failed to establish that the statement in *Hemispheres* is a term or condition of carriage.

***Issue 2      Is the statement in Hemispheres misleading contrary to section 18(b) of the ATR?***

The statement in *Hemispheres* is not misleading. The statement does not state that a term or condition of carriage is that passengers abide by the statement or that a consequence of non-compliance is removal from the aircraft or a refusal to transport the passenger.

While the statement does use strong language, such as the term “prohibit”, the use of this term does not mislead the reader to believe that compliance with the statement is a term or condition. Passengers are aware that all kinds of socially unacceptable behavior on an aircraft are prohibited by flight crew—e.g. singing, playing a harmonica, or reading another passenger's business papers. Moreover, passengers are aware that socially prohibited behavior is not in itself a ground for removal from the aircraft or a refusal to transport, but that disruptive behavior could result in such consequences. The statement simply provides explicit notice that certain socially unacceptable behavior that affects safety and security will be prohibited by flight crew during the flight.

For the reasons above, United submits that Lukács has failed not only to establish that the statement in *Hemispheres* is a term or condition of carriage, but also that it is misleading, and therefore Lukács's complaint that the statement in *Hemispheres* contravenes sections 18(b) and 111(1) of the ATR does not stand.



***Issue 3: Regardless of whether or not the statement is a term or condition of carriage, is it reasonable?***

United submits that if the statement in *Hemispheres* were a term or condition of carriage found in its Tariff, it would be reasonable pursuant to section 111(1) of the ATR.

***a) Legal Principles governing section 111(1) of the ATR***

If the statement in *Hemispheres* is a term or condition of carriage, the burden is on Lukács to establish that it is unreasonable. In Decision No. 613-C-A-2006, the Agency stated, “[...] when a complaint is filed with the Agency, the complainant has the burden of providing evidence to the Agency that the air carrier has applied a term or condition of carriage that is “unreasonable or unduly discriminatory” within the meaning of subsection 67.2(1) of the CTA and section 111 of the ATR”.<sup>13</sup> Thus, while there may be no presumption that a tariff is reasonable or unreasonable, the burden is upon Lukács, as the complainant, to establish on a balance of probabilities that the statement he alleges is a term or condition of carriage is unreasonable.

United agrees with Lukács that in determining whether or not a term or condition is reasonable, the Agency has consistently taken the position that it will balance the rights of passengers to be subject to reasonable terms and conditions of carriage, and the particular air carrier’s statutory, commercial and operational obligations.<sup>14</sup>

United submits that Lukács has failed to meet his burden of establishing that the alleged term and condition of carriage is unreasonable.

***b) Privacy and public policy: society’s privacy expectations as reflected in law***

United submits that the statement in *Hemispheres* would be reasonable if it were a term or condition of carriage, because it is a reflection of society’s broader privacy expectations and is consistent with broader public policy regarding the collection, use and disclosure of personal information.

Society highly values individuals’ right to privacy. This right to privacy includes the right of individuals’ to decide who collects their personal information, including through photography and video-recording, and how collected information may be used. Consequently, society expects that individuals’ activities will not be unnecessarily recorded without their consent except in limited and extenuating circumstances. This expectation of privacy is not limited to private activities or residences; rather, the expectation continues to exist even when individuals are at work or in public spaces.

---

<sup>13</sup> CTA Decision No. 613-C-A-2006

<sup>14</sup> CTA Interlocutory Decision No. LET-C-A-78-2011 at para 64.





Society's privacy expectations are reflected in Canadian legislation and common law. United submits that in determining whether the statement in *Hemispheres* would be reasonable if it were a term or condition of carriage, the Agency should consider the statement vis-a-vis society's privacy expectations including society's core privacy expectations which are reflected in law. In particular, the Agency should consider that the statement in *Hemispheres* is consistent with broader public policy underlying privacy laws. For illustration purposes, below is a brief summary of Canada's privacy laws.

*Privacy legislation – Government collection, use and disclosure of personal information*

Every Canadian province and the federal government have passed laws that protect the personal information collected, controlled and used by governments.<sup>15</sup> The Supreme Court of Canada has recognized the federal statute as “fundamental to the Canadian legal system” and “quasi-constitutional”, a view equally applicable to the provincial statutes.<sup>16</sup> The various pieces of legislation adopt a similar definition of “personal information”, namely, information about an identifiable individual.<sup>17</sup> It is universally accepted that photography and video and audio-recordings of an identifiable individual constitute the collection of personal information.<sup>18</sup>

The various statutes take a similar approach to protecting individuals' personal information. First, personal information may be collected only if it relates directly to the operation of a program or is authorized by law.<sup>19</sup> In other words, superfluous and unnecessary collection of personal information is prohibited, including video-recordings and photographs of individuals. Second, information may be used only for the purpose for which it was collected, unless the

---

<sup>15</sup> *Privacy Act*, RSC 1985, c P-21; *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5; *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01; *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31; *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56; *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6; *Access to Information and Protection of Privacy Act*, SNWT (Nu) 1994, c 20; *Access to Information and Protection of Privacy Act*, RSY 2002, c 1; *The Freedom of Information and Protection of Privacy Act*, CCSM c F175; *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1.

<sup>16</sup> *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 at para 24.

<sup>17</sup> For Example, see: *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5, s. 3(1)(i); *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s. 2(1)(c).

<sup>18</sup> Appendix G: Dr. Ann Cavoukian, “Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report“, Privacy Investigation Report MC07-68 (March 30, 2007) at 19-20; Appendix E: Privacy Commissioner of Canada, “Guidance on Covert Video Surveillance in the Private Sector” (May 2009); Appendix F: Information and Privacy Commissioner of Alberta, Privacy Commissioner of Canada, and Information and Privacy Commissioner for British Columbia, “Guidelines for Overt Video Surveillance in the Private Sector (March 2008)”.

<sup>19</sup> For example, see: *Privacy Act*, RSC 1985, c P-21, s. 4; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5, s. 24(1); *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s. 38(2).



individual associated with the information provides their consent.<sup>20</sup> Third, the personal information controlled by government shall not be disclosed without the consent of the individual to whom the information relates unless disclosure is specifically authorized by the statute.<sup>21</sup>

### *Privacy legislation – organizations*

Legislation also governs the collection of personal information by persons. In general, this type of legislation can be divided into two categories. The first is legislation dealing with personal health information. The second is information used by businesses.

Some provinces have passed legislation dealing specifically with personal health information.<sup>22</sup> Depending on the circumstances, these statutes may apply to governments, businesses and health care organizations. Thus, these statutes could apply to subjects that might ordinarily fall under the government-specific privacy acts discussed above (e.g. a government Minister) or it may apply to a business that would normally be subject to a statute like the *Personal Information and Protection of Electronic Documents Act* (“**PIPEDA**”).<sup>23</sup> In other provinces, personal health information is protected under PIPEDA, PIPEDA-equivalent legislation or government-specific privacy legislation, whichever is applicable in the circumstances.

Personal health information statutes extend the same principles found in governmental privacy laws to health professions, health facilities, public bodies and the like who collect and maintain individuals’ personal health information.<sup>24</sup> The various statutes define “personal health information” to mean, in general, identifying information about an individual’s health.<sup>25</sup> This information could include information about an individual’s health, the provision of health care to the individual, the individual’s eligibility for a health care program or a health benefit, non-

---

<sup>20</sup> For example, see: *Privacy Act*, RSC 1985, c P-21, s. 7; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5, s. 26; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s. 41(1).

<sup>21</sup> For example, see: *Privacy Act*, RSC 1985, c P-21, s. 8; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5, s. 27; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s. 42(1).

<sup>22</sup> *Personal Health Information Act*, SNL 2008, c P-7.01; *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c 38; *Personal Health Information Act*, CCSM c P33.5; *Personal Health Information Act*, SNS 2010, c 41 (Not yet in force); *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A; *The Health Information Protection Act*, SS 1999, c H-0.021

<sup>23</sup> *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [PIPEDA].

<sup>24</sup> See: *Personal Health Information Act*, SNL 2008, c P-7.01, ss. 29(1), 31-34, 36; *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A, ss. 29, 31, 37, 38; *Personal Health Information Act*, CCSM c P33.5, ss. 13, 21, 22.

<sup>25</sup> For example, see: *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s. 2; *Personal Health Information Act*, SNL 2008, c P-7.01, s. 5(1); *Personal Health Information Act*, CCSM c P33.5, s. 5(1).



health related personal information collected in the course of the provision of health care, prescription information, and registration information.<sup>26</sup>

All Canadian commercial organizations are also subject to laws governing the collection, use and disclosure of personal information. PIPEDA, a federal statute, applies to any organization, including an association, partnership, person or trade union, that collects, uses or discloses personal information in the course of commercial activities.<sup>27</sup> It also applies with respect to such organizations' collection, use and disclosure of personal information relating to employees where the operation is a federal work, undertaking or business.<sup>28</sup> Pursuant to section 26(2) of PIPEDA, provincially-enacted PIPEDA-equivalent legislation applies to organizations in Alberta, BC, and Quebec, in addition to health care professionals in Ontario, Newfoundland and Labrador and New Brunswick.<sup>29</sup> The Federal Court has recognized PIPEDA as a fundamental law of Canada.<sup>30</sup>

PIPEDA defines "personal information" as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization".<sup>31</sup> PIPEDA requires that organizations' collection, use and disclosure of personal information comply with a set of obligations appended to the statute.<sup>32</sup> Pursuant to these obligations, an organization collecting, using or disclosing personal information must:

- Have the individual's consent to collect, use and disclose personal information;
- Identify the purpose for which personal information is collected before or at the time it is collected;
- Limit the collection of personal information to that which is necessary for the purposes identified by the organization (i.e. collection cannot be indiscriminate)
- Only collect personal information by lawful and fair means;
- Only use and disclose collected information for the purposes for which it was collected (i.e. if an organization wants to use collected information for a purpose other than that identified at the time of collection it needs further consent from the individual);

---

<sup>26</sup>For example, see: *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s. 2; *Personal Health Information Act*, SNL 2008, c P-7.01, s. 5(1); *Personal Health Information Act*, CCSM c P33.5, s. 5(1).

<sup>27</sup> PIPEDA, s. 4(1).

<sup>28</sup> PIPEDA, s. 4(1).

<sup>29</sup> PIPEDA, s. 26(2); *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219; *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220; *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374; *Health Information Custodians in the Province of Ontario Exemption Order* SOR/2005-399; *Personal Health Information Custodians in New Brunswick Exemption Order*, SOR/2011-265; *Personal Health Information Custodians in Newfoundland and Labrador Exemption Order*, SI/2012-72.

<sup>30</sup> *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 at para 100.

<sup>31</sup> PIPEDA, s. 2. PIPEDA defines "personal health information" similar to provincial statutes discussed above.

<sup>32</sup> PIPEDA, s. 5(1). These obligations are subject to section 6 through 9 of the Act.



- Destroy collected personal information that is no longer required in order to fulfill the purpose for which it was collected; and
- Adequately protect personal information from unauthorized access, use and disclosure.

In addition to these obligations, PIPEDA requires that an organization “collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances”.<sup>33</sup> The Federal Privacy Commissioner has employed a four-part test to determine reasonableness which has been adopted by the Federal Court. In determining reasonableness, the Commissioner will consider: 1) is the measure demonstrably necessary to meet a specific need?; 2) is it likely to be effective in meeting that need? 3) is the loss of privacy proportional to the benefit gained?; and 4) is there a less privacy-intrusive way of achieving the same end?<sup>34</sup>

The Federal Court has jurisdiction to award damages for a breach of PIPEDA.<sup>35</sup>

As discussed above, Alberta, British Columbia and Quebec have laws that are substantively similar to PIPEDA and organizations subject to these statutes are exempt from PIPEDA.<sup>36</sup> Like PIPEDA, the Alberta and British Columbia provincial acts require that organizations meet particular obligations and that their collection, use and disclosure of information be reasonable.<sup>37</sup>

#### *Privacy Law – Torts*

The invasion of an individual’s privacy is an actionable tort in many Canadian jurisdictions . In British Columbia, Newfoundland and Labrador, Saskatchewan, and Manitoba the legislatures have recognized that the willful violation of another individual’s privacy is an actionable tort even without proof of damage.<sup>38</sup> These legislatures have also seen it fit to specify that a tortious

---

<sup>33</sup> PIPEDA, s. 5(3).

<sup>34</sup> *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 at para 126; Video surveillance cameras at food processing plant questioned, PIPEDA Case Summary #290 (January 27, 2005), 2005 CanLII 15490 (PCC); Employee objects to company’s use of digital video surveillance cameras, PIPEDA Case Summary #114 (January 23, 2003), 2003 CanLII 40422 (PCC) ; Bus terminal video surveillance is challenged by company employee, PIPEDA Case Summary #2009-001 (February 19, 2009), 2009 CanLII 49329 (PCC); Transit driver objects to use of technology (MDT and GPS) on company vehicle, PIPEDA Case Summary #2009-011 (May 27, 2009), 2009 CanLII 74728 (PCC); Law School Admission Council Investigation, PIPEDA Case Summary #2008-389 (May 29, 2008), 2008 CanLII 28249 (PCC); Use of personal information collected by Global Positioning System considered, PIPEDA Case Summary #351 (November 9, 2006), 2006 CanLII 42313 (PCC).

<sup>35</sup> PIPEDA, s 16(c).

<sup>36</sup> PIPEDA, s. 26(2); *Personal Information Protection Act*, S.A. 2003, c. P-6; *Personal Information Protection Act*, S.B.C. 2003, c. 63; *An Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1.

<sup>37</sup> *Personal Information Protection Act*, S.A. 2003, c. P-6, s. 5(5); *Personal Information Protection Act*, SBC 2003, c 63, s. 11.

<sup>38</sup> *Privacy Act*, RSBC 1996, c 373, s. 1(1). *Privacy Act*, RSNL 1990, c P-22, s. 3; *The Privacy Act*, RSS 1978, c P-24, s. 2; *The Privacy Act*, CCSM c P125, s. 2.



violation of privacy may occur by eavesdropping or surveillance regardless of whether the act is accomplished by trespassing.<sup>39</sup> In other words, an individual could be liable for eavesdropping on a conversation or video-recording another individual in a public space.

In other jurisdictions where no similar statute has been enacted, the Courts have recognized a common law tort for invasion of privacy. For example, in *Jones v. Tsige*, the Ontario Court of Appeal recognized the tort of intrusion upon seclusion.<sup>40</sup> The court held that the elements of the tort are the same as those espoused in the *Restatement (Second) of Torts* (2010), namely, “One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person”.<sup>41</sup>

#### *Privacy law – Criminal Code*

Canada’s Criminal Code also regulates privacy. Pursuant to section 184(1) of the Criminal Code, “Everyone who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”. The Code defines “private communication” to mean an oral communication or telecommunication “[...] that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it [...]”.<sup>42</sup> The Supreme Court of Canada has held that “It will be observed at once that under the definition of “private communication” it is the originator’s state of mind that is decisive”.<sup>43</sup> United submits that a “private communication” may occur between two individuals who are within close proximity of other individuals.

#### *Summary*

Society has many norms governing the relations and interactions between individuals. Many are not codified. For example, there are no laws against being rude or unkind and there is no actionable tort for being an unpleasant person. There are, however, social consequences for such inappropriate behavior, e.g. social isolation or loss of employment. On the other hand, some behaviors are viewed by society as sufficiently offensive or problematic to warrant legal regulation. Thus, while an individual may be rude to his neighbor, he cannot threaten her, trespass on her property, vandalize her car or cause a nuisance.

---

<sup>39</sup> *Privacy Act*, RSBC 1996, c 373, s. 1(3); *The Privacy Act*, RSS 1978, c P-24, s. 3; *Privacy Act*, RSNL 1990, c P-22, s. 4; *The Privacy Act*, CCSM c P125, s. 3;

<sup>40</sup> *Jones v. Tsige*, 2012 ONCA 32 at para 65.

<sup>41</sup> *Jones v. Tsige*, 2012 ONCA 32 at para 70.

<sup>42</sup> *Criminal Code*, R.S.C., 1985, c. C-46, s. 183

<sup>43</sup> *Goldman v. R.*, [1980] 1 SCR 976 at 992.



The fact that Canada has extensive privacy laws shows that Canada has very high privacy expectations and that it views the non-consensual collection of personal information, even in public places, as highly offensive. These privacy laws—whether judicially recognized or legislatively enacted—provide credible evidence of society’s privacy expectations. In deciding whether or not the statement in *Hemispheres* would be reasonable if it were a term or condition of carriage, the Agency should evaluate the statement against societal norms and expectations which manifest in our legal system.

Statutes governing the collection, use and disclosure of individuals’ personal information by governments, health care providers and organizations in various Canadian jurisdictions provides that the collection of personal information may only occur with the individual’s consent or if it is specifically authorized by law, that the collection of personal information must be limited, that governments and organizations may use the information only for the purpose for which it was collected and that the government or organization cannot disclose the information unless the individual consents to the disclosure or the disclosure is authorized by statute. These principles, reflected across Canada’s federal and provincial jurisdictions, demonstrate that society is protective of individual’s personal information. In particular, they illustrate society’s view that individuals have a right to privacy and a right to control how their personal information is collected, used and disclosed. Further, they illustrate society’s expectation that except in limited circumstances authorized by law, personal information may only be collected, used, and disclosed with the consent of the individual and only for the purposes for which the information was originally collected. United submits that when evaluating the reasonableness of the statement in *Hemispheres*, it is important to consider the statement against society’s expectations as reflected in these types of statutes and the common law.

***a) The statement is reasonable***

The statement in *Hemispheres* includes four elements. 1) Passengers are welcome to record their personal events; 2) Passenger’s may record other passengers only with the latter’s prior consent; 3) Passengers may not record flight crews without permission; and 4) Passengers may not record United equipment and procedures without permission. United submits that each element, and the statement as a whole, is reasonable.

*Personal Events*

United submits that permitting passengers to record their “personal events” is reasonable and that the term is sufficiently clear. It is impractical, if not impossible, to draft a statement that clearly recognizes every possible circumstance or case where the recording of an undefinable number of potential events unique and personal to a passenger would be reasonable. As such, United sought a term that provided a sufficiently clear guide as to what subject matter could be recorded on a case by case basis. United submits that the term “personal events” meets this objective. The term “personal events” is sufficiently clear to provide passengers and crew with a fair, objective and reasonable means of determining what type of events and subject matter an individual may record while on board an aircraft. This is particularly so when the term “personal events” is read

with the rest of the statement including the prohibition on recording other passengers, crew, and United equipment and procedures without proper consent or authorization.

*Recording other passengers without their consent*

A prohibition on the recording other passengers without their consent is reasonable.

First, while people have lower expectations of privacy in public spaces than they do in private spaces, they do maintain expectations of privacy when in public. An individual's presence in a public space does not mean governments or organizations have an unfettered right to record or photograph them.<sup>44</sup> The Federal Privacy Commissioner has made it clear that PIPEDA applies to photographs and videos of identifiable individuals in public spaces and that the collection of individuals' images in public for a commercial purpose must comply with PIPEDA.<sup>45</sup> Similarly, the Ontario Privacy Commissioner's thorough investigation of video-recording surveillance in mass transit systems emphasizes the importance of protecting individuals' personal information and individuals' expectations of privacy while travelling on public transit even when the collection of personal information in public spaces is legitimately required for public safety and security.<sup>46</sup> Individuals also do not forego their privacy expectations when in a private business or a place of employment. Video-recordings of customers must comply with applicable legislation, and unnecessary or unreasonable recordings are prohibited.<sup>47</sup> Likewise, an employer cannot video-record employees "just because".<sup>48</sup>

Aircrafts are unique environments. In a globalized world, air travel is an essential means of transportation. Given the expense of operating an aircraft, the majority of those who use air transportation must use commercial carriers. Within these commercial carriers, passengers are assigned a relatively limited amount of space which they must occupy for the duration of the flight. Passengers are not able to choose who will sit within proximity of them and passengers have no right to move away from another passenger. While passengers may be in close proximity to each other, passengers do maintain expectations of privacy. They expect that other passengers will not look at their papers or computer, that they will not have to divulge personal information to other passengers, that other passengers will not disrupt their peace, that other passengers will

---

<sup>44</sup> Appendix G: Dr. Ann Cavoukian, "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report", Privacy Investigation Report MC07-68 (March 30, 2007) at 2.

<sup>45</sup> Appendix H: Transcript of the Office of the Privacy Commissioner's Appearance before the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Privacy Implications of Camera Surveillance, October 22, 2009, Ottawa, Ontario.

<sup>46</sup> Appendix G: Dr. Ann Cavoukian, "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report", Privacy Investigation Report MC07-68 (March 30, 2007) at 2.

<sup>47</sup> PIPEDA, s. 5(3); PIPEDA, Schedule 1. Appendix F: Information and Privacy Commissioner of Alberta, Privacy Commissioner of Canada, and Information and Privacy Commissioner for British Columbia, "Guidelines for Overt Video Surveillance in the Private Sector (March 2008)".

<sup>48</sup> *Eastmond v. Canadian Pacific Railway*, 2004 FC 852.



respect the assigned spaces, and that other passengers will not interfere with their property. Further, United submits that passengers expect that they will not be recorded while on an aircraft. Passengers would find it highly intrusive and offensive to be filmed or photographed while eating, while reading, while sleeping, while entering and leaving a lavatory, or while discussing private matters with a flight attendant or another passenger. The fact that others may observe these activities by virtue of their physical proximity does not give them a right to record them and then use and distribute the record of the event as they see fit. As such, while passengers may have lower expectations of privacy on an aircraft than in their residence, they still maintain privacy expectations and, in United's view, they reasonably expect not to be recorded by other passengers without their consent. Moreover, individuals and companies can prohibit or restrict the use of photography on private property and many businesses do so for the comfort of their customers and employees.

The Agency has also previously recognized that carriers have an obligation to ensure passenger privacy. For example, in Decision No. 290-AT-A-2000, the Agency determined that a carrier's failure to follow its procedures, including the installation of a privacy curtain around a passenger being transported on a stretcher, left the passenger humiliated and embarrassed and constituted an undue obstacle to the passenger's mobility. In other words, the Agency requires carriers to ensure that a passenger's privacy vis-à-vis other passengers is appropriately afforded.

Second, in some circumstances a photograph or video-recording of an individual is prohibited or restricted by law. For example, PIPEDA and similar legislation applies to photographs and video-recordings of identifiable individuals in public spaces. As such, if a person takes a video or photograph of an individual for a commercial purpose, then consent is required for the collection, use or disclosure of the photograph or video.

In addition, the video-recording or photography of another individual may result in civil or criminal liability. Depending on the circumstances, a video-recording or photography of another individual could result in tort liability under the British Columbia, Manitoba, Saskatchewan or Newfoundland and Labrador statutes or under the common law or could result in damages under PIPEDA. Furthermore, the recording of other individuals' conversations could be a criminal offence if the discussing parties had a reasonable expectation that their conversation was private. United submits that the prohibition on video-recording and photography of other passengers is reasonable because it is consistent with the public policy underlying Canada's legal regulation of privacy.

Third, a passenger's interest in documenting a potential event involving another passenger is neither demonstrably necessary to meet a specific need nor is the resulting loss of privacy proportional to the benefit gained. Given the confines of an aircraft, events between passengers and/or crew usually occur in the presence of multiple witnesses. These witness accounts provide objective and credible evidence of the events. The loss of privacy resulting from a rule that passengers have a right to photograph and record other passengers far outweighs any evidentiary benefit from recording a potential event that may occur at some point in the future.





Fourth, other airlines have similarly decided to include a statement in their onboard magazine which provides passengers with notice that it is inappropriate to photograph or video-record other passengers without consent.<sup>49</sup>

In summary, forbidding the recording of other passengers is reasonable and consistent with public policy regarding the collection of individual's personal information.

*Forbidding the recording of crew*

To determine the reasonableness of a requirement that passengers obtain consent to photograph or video-record flight crew, the Agency should consider society's broader expectations of privacy in the workplace. While individuals may have lower expectations of privacy in the workplace, they do not completely forego their privacy interests. This view is supported by the fact that PIPEDA and other provincial legislation apply to many employment relationships.

United submits that a prohibition on the video-recording or photography of flight crew without consent is reasonable.

First, the flight crew have a reasonable expectation of some privacy while working. The recording of crew collects more than just information about the individuals in their professional capacity; it also collects personal information.<sup>50</sup> As individuals, flight crew should not be forcefully subjected to photography and video-recording by customers while working by virtue of the fact they are employed by an airline. No waiter in a restaurant would expect that customers could rightfully video-record them without their consent simply because they are seated in the restaurant. In some circumstances flight attendants and waiters may feel comfortable being photographed or video-recorded by a passenger or customer. In such circumstances, the recording of personal information should occur only with the consent of flight attendant or waiter and only if the employer does not have a reasonable objection to the recording in the workplace.

Second, forced subjection to video-recording and photographs is demeaning and humiliating. Providing passengers with an unfettered right to video-record flight crew treats flight crew as untrustworthy suspects and objects on display for passengers. Allowing the non-consensual recording of flight crew treats flight crew in a non-dignified manner.

Third, it has been recognized that subjecting employees to video-recording is preoccupying.<sup>51</sup> It could cause flight crew to focus on when and how they are being recorded in a particular situation and thereby distract their attention from a situation at hand or their duties. Alternatively, it could dissuade crew from attending to a situation out of a fear of being recorded. In either case, it could affect the safety and security of the flight.

---

<sup>49</sup> Appendix C: *American Way* (April 1, 2013), p. 80.

<sup>50</sup> *Halton Regional Police Services Board (Re)*, IPC Interim Order MO-2606-I (March 24, 2011), 2011 CanLII 16661 (ON IPC).

<sup>51</sup> *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 at para 159; *Hoffman* at 50.



Fourth, for the reasons discussed above, in some circumstances the video-recording or photography of crew may be contrary to privacy laws.

Fifth, other airlines have similarly decided to include a statement in their onboard magazine which provides passengers with notice that it is inappropriate to photograph or video-record other flight crew without consent.<sup>52</sup>

Sixth, Lukács has provided no evidence that it is demonstrably necessary for passengers to video-record or photograph flight crew, that the benefits gained from allowing passengers to photograph or video-record flight crew is proportionate to the loss of privacy or that there is no less privacy intrusive means of addressing the issues he claims justify the video-recording and photograph of crew.

Lukács claims that video-recording and photography of flight crew is “an important tool for passengers to defend themselves against abusive conduct and against groundless allegations of misconduct that are so frequently leveled against passengers”.<sup>53</sup> Lukács has provided no evidence of frequent abuse and frequent groundless allegations against passengers, an allegation that United disputes. United submits that issues with passenger behavior are rare and that it is even more rare for there to be a fundamental disagreement of the facts associated with the event. The fact that a member of a flight crew and a passenger may have different recollections of an event does not mean it is demonstrably necessary for passengers to have the right to video-record a flight crew at all times. Unlike a telephone conversation, other persons are physically present on an aircraft. Objective factual evidence of the event can be gathered from those present, including other passengers and flight crew. This is a far less privacy-intrusive method of determining what occurred in those rare circumstances where there is a factual dispute. Moreover, the benefits of having the right to video-record flight crew in the rare event of an onboard event does not outweigh the severe privacy impacts of allowing passengers to film flight crew at all times.

United submits that for the above reasons, the prohibition on video-recording and photograph of flight crew without consent is consistent with public policy and is reasonable.

*Forbidding the video-recording of United equipment and procedures*

There are three reasons for prohibiting the unauthorized photography and video-recording of United equipment, including the interior of the aircraft, and United procedures. The first reason is the safety and security of the aircraft. Various procedures are employed throughout a flight to ensure its safety and security. While some of these are overt—such as the safety demonstration at the beginning of the flight—others are not. United is conscious of the fact that a key component to the 9/11 terrorist attacks was the surveillance of flight crew procedures and airline

---

<sup>52</sup> Appendix C: *American Way* (April 1, 2013), p. 80.

<sup>53</sup> Lukács Complaint, dated February 24, 2013 at 4.



equipment.<sup>54</sup> There is no way of knowing if passengers filming United equipment and procedures will have an ill intent. Nonetheless, United feels that it is in the interest of safety and security that certain procedures not be recorded and distributed online where they can be studied. Given that United does not want to draw attention to certain of those procedures and equipment, it has decided to prohibit the unauthorized recording of procedures and equipment broadly. That said, flight crew have discretion and are unlikely to request that a passenger stop filming United equipment or procedures on the basis of safety and security if the subject matter captured is benign or incidental to the recording of personal events, unless certain procedures or equipment are also being captured.

Second, the design of aircraft makes it very difficult to record the interior of the aircraft without recording personal information of other passengers and crew. Requiring authorization to record the interior of an aircraft is a reasonable and appropriate means of protecting passengers' and flight crew's privacy.

Third, other airlines have similarly decided to include a statement in their onboard magazine which provides passengers with notice that it is inappropriate to photograph or video-record other airline procedures and equipment without authorization.<sup>55</sup>

Lastly, business operators have the right to control photography and video-recording inside their place of business. Returning to the restaurant example, an operator of a restaurant would have no issue with a customer taking a picture of their companion inside the restaurant. Conversely, it would be perfectly reasonable for a restaurant operator to ask a customer wandering the restaurant while filming its interior to stop. Similarly, the inside of an aircraft is United's private property and it is reasonable for United to prohibit passengers from video-recording the interior without authorization.

## Conclusion

For the reasons set out above, United submits that the Agency should dismiss Lukács's complaint. The statement appearing in *Hemispheres* is not a term or condition of carriage and does not belong within United's Tariff. United does not treat the statement as a term or condition of carriage and United does not refuse carriage or remove passengers solely for acting contrary to the statement.

Further, the statement is not misleading. While the statement uses the term "prohibit", neither the statement nor the context in which it appears in *Hemispheres* misleads passengers to believe that the statement is a term or condition of carriage.

---

<sup>54</sup> Appendix A: National Commission on Terrorist Attacks, The 9/11 Commission Report at 242, 243, 245, 248, available at <http://www.9-11commission.gov/report/911Report.pdf>.

<sup>55</sup> Appendix C: *American Way* (April 1, 2013), p. 80.



The statement in *Hemispheres* is reasonable. It reflects society's expectations regarding video-recording and photography on aircraft and balances individuals' interest in recording their personal events with other passengers' privacy expectations, flight crews' privacy expectations, United's right to ensure the comfort and dignity of its customers and employees and the need to ensure safety and security of the aircraft. Further, it is consistent with current public policy.

Lastly, United submits that this response adequately addresses Lukács's questions.

Yours truly,

Drew Tyler

cc: Dr. Gábor Lukács

Jeff Wittig, United Airlines', Senior Counsel-Asia/Pacific

## LIST OF ATTACHMENTS

- Appendix A:** National Commission on Terrorist Attacks, The 9/11 Commission Report at 242, 243, 245, 248, available at <http://www.9-11commission.gov/report/911Report.pdf>
- Appendix B:** Hemispheres Magazine, August 2012 at 129.
- Appendix C:** American Way (April 1, 2013), p. 80.
- Appendix D:** Dictionary pages
- Appendix E:** Privacy Commissioner of Canada, “Guidance on Covert Video Surveillance in the Private Sector” (May 2009)
- Appendix F:** Information and Privacy Commissioner of Alberta, Privacy Commissioner of Canada, and Information and Privacy Commissioner for British Columbia, “Guidelines for Overt Video Surveillance in the Private Sector (March 2008)”
- Appendix G:** Dr. Ann Cavoukian, “Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report“, Privacy Investigation Report MC07-68 (March 30, 2007)
- Appendix H:** Transcript of the Office of the Privacy Commissioner’s Appearance before the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Privacy Implications of Camera Surveillance, October 22, 2009, Ottawa, Ontario

**Appendix A:**

National Commission on Terrorist Attacks,  
The 9/11 Commission Report at 242, 243, 245,  
248, available at

[http://www.9-  
11commission.gov/report/911Report.pdf](http://www.9-11commission.gov/report/911Report.pdf)

THE 9/11  
COMMISSION  
REPORT

# CONTENTS

*List of Illustrations and Tables ix*

*Member List xi*

*Staff List xiii–xiv*

*Preface xv*

1. “WE HAVE SOME PLANES” 1
  - 1.1 Inside the Four Flights 1
  - 1.2 Improvising a Homeland Defense 14
  - 1.3 National Crisis Management 35
  
2. THE FOUNDATION OF THE NEW TERRORISM 47
  - 2.1 A Declaration of War 47
  - 2.2 Bin Ladin’s Appeal in the Islamic World 48
  - 2.3 The Rise of Bin Ladin and al Qaeda (1988–1992) 55
  - 2.4 Building an Organization, Declaring  
War on the United States (1992–1996) 59
  - 2.5 Al Qaeda’s Renewal in Afghanistan (1996–1998) 63
  
3. COUNTERTERRORISM EVOLVES 71
  - 3.1 From the Old Terrorism to the New:  
The First World Trade Center Bombing 71
  - 3.2 Adaptation—and Nonadaptation—  
in the Law Enforcement Community 73
  - 3.3 . . . and in the Federal Aviation Administration 82
  - 3.4 . . . and in the Intelligence Community 86



3.5	... and in the State Department and the Defense Department	93
3.6	... and in the White House	98
3.7	... and in the Congress	102
4.	RESPONSES TO AL QAEDA'S INITIAL ASSAULTS	108
4.1	Before the Bombings in Kenya and Tanzania	108
4.2	Crisis: August 1998	115
4.3	Diplomacy	121
4.4	Covert Action	126
4.5	Searching for Fresh Options	134
5.	AL QAEDA AIMS AT THE AMERICAN HOMELAND	145
5.1	Terrorist Entrepreneurs	145
5.2	The "Planes Operation"	153
5.3	The Hamburg Contingent	160
5.4	A Money Trail?	169
6.	FROM THREAT TO THREAT	174
6.1	The Millennium Crisis	174
6.2	Post-Crisis Reflection: Agenda for 2000	182
6.3	The Attack on the USS <i>Cole</i>	190
6.4	Change and Continuity	198
6.5	The New Administration's Approach	203
7.	THE ATTACK LOOMS	215
7.1	First Arrivals in California	215
7.2	The 9/11 Pilots in the United States	223
7.3	Assembling the Teams	231
7.4	Final Strategies and Tactics	241
8.	"THE SYSTEM WAS BLINKING RED"	254
8.1	The Summer of Threat	254
8.2	Late Leads—Mihdhar, Moussaoui, and KSM	266
9.	HEROISM AND HORROR	278
9.1	Preparedness as of September 11	278
9.2	September 11, 2001	285
9.3	Emergency Response at the Pentagon	311
9.4	Analysis	315

10. WARTIME	325
10.1 Immediate Responses at Home	326
10.2 Planning for War	330
10.3 “Phase Two” and the Question of Iraq	334
11. FORESIGHT—AND HINDSIGHT	339
11.1 Imagination	339
11.2 Policy	348
11.3 Capabilities	350
11.4 Management	353
12. WHAT TO DO? A GLOBAL STRATEGY	361
12.1 Reflecting on a Generational Challenge	361
12.2 Attack Terrorists and Their Organizations	365
12.3 Prevent the Continued Growth of Islamist Terrorism	374
12.4 Protect against and Prepare for Terrorist Attacks	383
13. HOW TO DO IT? A DIFFERENT WAY OF ORGANIZING THE GOVERNMENT	399
13.1 Unity of Effort across the Foreign-Domestic Divide	400
13.2 Unity of Effort in the Intelligence Community	407
13.3 Unity of Effort in Sharing Information	416
13.4 Unity of Effort in the Congress	419
13.5 Organizing America’s Defenses in the United States	423
<i>Appendix A: Common Abbreviations</i>	429
<i>Appendix B: Table of Names</i>	431
<i>Appendix C: Commission Hearings</i>	439
<i>Notes</i>	449

## LIST OF ILLUSTRATIONS AND TABLES

p. 15	FAA Air Traffic Control Centers
p. 15	Reporting structure, Northeast Air Defense Sector
p. 32–33	Flight paths and timelines
p. 49	Usama Bin Ladin
p. 64	Map of Afghanistan
p. 148	Khalid Sheikh Mohammed
p. 238–239	The 9/11 hijackers
p. 279	The World Trade Center Complex as of 9/11
p. 284	The World Trade Center radio repeater system
p. 288	The World Trade Center North Tower stairwell with deviations
p. 312	The Twin Towers following the impact of American Airlines Flight 11 and United Airlines Flight 175
p. 313	The Pentagon after being struck by American Airlines Flight 77
p. 313	American Airlines Flight 93 crash site, Shanksville, Pennsylvania
p. 413	Unity of effort in managing intelligence



## COMMISSION MEMBERS

Handwritten signature of Thomas H. Kean in black ink.

Thomas H. Kean

CHAIR

Handwritten signature of Lee H. Hamilton in black ink.

Lee H. Hamilton

VICE CHAIR

Handwritten signature of Richard Ben-Veniste in black ink.

Richard Ben-Veniste

Handwritten signature of Bob Kerrey in black ink.

Bob Kerrey

Handwritten signature of Fred F. Fielding in black ink.

Fred F. Fielding

Handwritten signature of John F. Lehman in black ink.

John F. Lehman

Handwritten signature of Jamie S. Gorelick in black ink.

Jamie S. Gorelick

Handwritten signature of Timothy J. Roemer in black ink.

Timothy J. Roemer

Handwritten signature of Slade Gorton in black ink.

Slade Gorton

Handwritten signature of James R. Thompson in black ink.

James R. Thompson

lacked visas; they returned to Florida that same day. They likely took this trip to renew Suqami's immigration status, as Suqami's legal stay in the United States ended May 21.<sup>131</sup>

On July 30, Shehri traveled alone from Fort Lauderdale to Boston. He flew to San Francisco the next day, where he stayed one night before returning via Las Vegas. While this travel may have been a casing flight—Shehri traveled in first class on the same type of aircraft he would help hijack on September 11 (a Boeing 767) and the trip included a layover in Las Vegas—Shehri was neither a pilot nor a plot leader, as were the other hijackers who took surveillance flights.<sup>132</sup>

The three Hamburg pilots—Atta, Shehhi, and Jarrah—took the first of their cross-country surveillance flights early in the summer. Shehhi flew from New York to Las Vegas via San Francisco in late May. Jarrah flew from Baltimore to Las Vegas via Los Angeles in early June. Atta flew from Boston to Las Vegas via San Francisco at the end of June. Each traveled in first class, on United Airlines. For the east-west transcontinental leg, each operative flew on the same type of aircraft he would pilot on September 11 (Atta and Shehhi, a Boeing 767; Jarrah, a Boeing 757).<sup>133</sup> Hanjour and Hazmi, as noted below, took similar cross-country surveillance flights in August.

Jarrah and Hanjour also received additional training and practice flights in the early summer. A few days before departing on his cross-country test flight, Jarrah flew from Fort Lauderdale to Philadelphia, where he trained at Hortman Aviation and asked to fly the Hudson Corridor, a low-altitude “hallway” along the Hudson River that passes New York landmarks like the World Trade Center. Heavy traffic in the area can make the corridor a dangerous route for an inexperienced pilot. Because Hortman deemed Jarrah unfit to fly solo, he could fly this route only with an instructor.<sup>134</sup>

Hanjour, too, requested to fly the Hudson Corridor about this same time, at Air Fleet Training Systems in Teterboro, New Jersey, where he started receiving ground instruction soon after settling in the area with Hazmi. Hanjour flew the Hudson Corridor, but his instructor declined a second request because of what he considered Hanjour's poor piloting skills. Shortly thereafter, Hanjour switched to Caldwell Flight Academy in Fairfield, New Jersey, where he rented small aircraft on several occasions during June and July. In one such instance on July 20, Hanjour—likely accompanied by Hazmi—rented a plane from Caldwell and took a practice flight from Fairfield to Gaithersburg, Maryland, a route that would have allowed them to fly near Washington, D.C. Other evidence suggests that Hanjour may even have returned to Arizona for flight simulator training earlier in June.<sup>135</sup>

There is no indication that Atta or Shehhi received any additional flight training in June. Both were likely too busy organizing the newly arrived muscle hijackers and taking their cross-country surveillance flights. Atta, moreover, needed to coordinate with his second-in-command, Nawaf al Hazmi.<sup>136</sup>

Although Atta and Hazmi appear to have been in Virginia at about the same time in early April, they probably did not meet then. Analysis of late April communications associated with KSM indicates that they had wanted to get together in April but could not coordinate the meeting.<sup>137</sup> Atta and Hazmi probably first met in the United States only when Hazmi traveled round-trip from Newark to Miami between June 19 and June 25.

After he returned to New Jersey, Hazmi's behavior began to closely parallel that of the other hijackers. He and Hanjour, for instance, soon established new bank accounts, acquired a mailbox, rented cars, and started visiting a gym. So did the four other hijackers who evidently were staying with them in New Jersey. Several also obtained new photo identification, first in New Jersey and then at the Virginia Department of Motor Vehicles, where Hazmi and Hanjour had obtained such documents months earlier, likely with help from their Jordanian friend, Rababah.<sup>138</sup>

Atta probably met again with Hazmi in early July. Returning from his initial cross-country surveillance flight, Atta flew into New York. Rather than return immediately to Florida, he checked into a New Jersey hotel. He picked up tickets to travel to Spain at a travel agency in Paterson on July 4 before departing for Fort Lauderdale. Now that the muscle hijackers had arrived, he was ready to meet with Ramzi Binalshibh for the last time.<sup>139</sup>

### **The Meeting in Spain**

After meeting with Atta in Berlin in January 2001, Binalshibh had spent much of the spring of 2001 in Afghanistan and Pakistan, helping move the muscle hijackers as they passed through Karachi. During the Berlin meeting, the two had agreed to meet later in the year in Kuala Lumpur to discuss the operation in person again. In late May, Binalshibh reported directly to Bin Ladin at an al Qaeda facility known as "Compound Six" near Kandahar.<sup>140</sup>

Bin Ladin told Binalshibh to instruct Atta and the others to focus on their security and that of the operation, and to advise Atta to proceed as planned with the targets discussed before Atta left Afghanistan in early 2000—the World Trade Center, the Pentagon, the White House, and the Capitol. According to Binalshibh, Bin Ladin said he preferred the White House over the Capitol, asking Binalshibh to confirm that Atta understood this preference. Binalshibh says Bin Ladin had given the same message to Waleed al Shehri for conveyance to Atta earlier that spring. Binalshibh also received permission to meet Atta in Malaysia. Atef provided money for the trip, which KSM would help Binalshibh arrange in Karachi.<sup>141</sup>

In early June, Binalshibh traveled by taxi from Kandahar to Quetta, Pakistan, where al Qaeda courier Abu Rahmah took him to KSM. According to Binalshibh, KSM provided a plane ticket to Malaysia and a fraudulent Saudi passport to use for the trip. KSM told him to ask Atta to select a date for the attacks. Binalshibh was to return to Germany and then inform KSM of the date. KSM

also gave Binalshibh the email address of Zacarias Moussaoui for future contact. Binalshibh then left for Kuala Lumpur.<sup>142</sup>

Binalshibh contacted Atta upon arriving in Malaysia and found a change in plan. Atta could not travel because he was too busy helping the new arrivals settle in the United States. After remaining in Malaysia for approximately three weeks, Binalshibh went to Bangkok for a few days before returning to Germany. He and Atta agreed to meet later at a location to be determined.<sup>143</sup>

In early July, Atta called Binalshibh to suggest meeting in Madrid, for reasons Binalshibh claims not to know. He says he preferred Berlin, but that he and Atta knew too many people in Germany and feared being spotted together. Unable to buy a ticket to Madrid at the height of the tourist season, Binalshibh booked a seat on a flight to Reus, near Barcelona, the next day. Atta was already en route to Madrid, so Binalshibh phoned Shehhi in the United States to inform him of the change in itinerary.<sup>144</sup>

Atta arrived in Madrid on July 8. He spent the night in a hotel and made three calls from his room, most likely to coordinate with Binalshibh. The next day, Atta rented a car and drove to Reus to pick up Binalshibh; the two then drove to the nearby town of Cambrils. Hotel records show Atta renting rooms in the same area until July 19, when he returned his rental car in Madrid and flew back to Fort Lauderdale. On July 16, Binalshibh returned to Hamburg, using a ticket Atta had purchased for him earlier that day. According to Binalshibh, they did not meet with anyone else while in Spain.<sup>145</sup>

Binalshibh says he told Atta that Bin Ladin wanted the attacks carried out as soon as possible. Bin Ladin, Binalshibh conveyed, was worried about having so many operatives in the United States. Atta replied that he could not yet provide a date because he was too busy organizing the arriving hijackers and still needed to coordinate the timing of the flights so that the crashes would occur simultaneously. Atta said he required about five to six weeks before he could provide an attack date. Binalshibh advised Atta that Bin Ladin had directed that the other operatives not be informed of the date until the last minute. Atta was to provide Binalshibh with advance notice of at least a week or two so that Binalshibh could travel to Afghanistan and report the date personally to Bin Ladin.<sup>146</sup>

As to targets, Atta understood Bin Ladin's interest in striking the White House. Atta said he thought this target too difficult, but had tasked Hazmi and Hanjour to evaluate its feasibility and was awaiting their answer. Atta said that those two operatives had rented small aircraft and flown reconnaissance flights near the Pentagon. Atta explained that Hanjour was assigned to attack the Pentagon, Jarrah the Capitol, and that both Atta and Shehhi would hit the World Trade Center. If any pilot could not reach his intended target, he was to crash the plane. If Atta could not strike the World Trade Center, he planned to crash his aircraft directly into the streets of New York. Atta told Binalshibh that each pilot had volunteered for his assigned target, and that the assignments were subject to change.<sup>147</sup>

During the Spain meeting, Atta also mentioned that he had considered targeting a nuclear facility he had seen during familiarization flights near New York—a target they referred to as “electrical engineering.” According to Binalshibh, the other pilots did not like the idea. They thought a nuclear target would be difficult because the airspace around it was restricted, making reconnaissance flights impossible and increasing the likelihood that any plane would be shot down before impact. Moreover, unlike the approved targets, this alternative had not been discussed with senior al Qaeda leaders and therefore did not have the requisite blessing. Nor would a nuclear facility have particular symbolic value. Atta did not ask Binalshibh to pass this idea on to Bin Ladin, Atef, or KSM, and Binalshibh says he did not mention it to them until after September 11.<sup>148</sup>

Binalshibh claims that during their time in Spain, he and Atta also discussed how the hijackings would be executed. Atta said he, Shehhi, and Jarrah had encountered no problems carrying box cutters on cross-country surveillance flights. The best time to storm the cockpit would be about 10–15 minutes after takeoff, when the cockpit doors typically were opened for the first time. Atta did not believe they would need any other weapons. He had no firm contingency plan in case the cockpit door was locked. While he mentioned general ideas such as using a hostage or claiming to have a bomb, he was confident the cockpit doors would be opened and did not consider breaking them down a viable idea. Atta told Binalshibh he wanted to select planes departing on long flights because they would be full of fuel, and that he wanted to hijack Boeing aircraft because he believed them easier to fly than Airbus aircraft, which he understood had an autopilot feature that did not allow them to be crashed into the ground.<sup>149</sup>

Finally, Atta confirmed that the muscle hijackers had arrived in the United States without incident. They would be divided into teams according to their English-speaking ability. That way they could assist each other before the operation and each team would be able to command the passengers in English. According to Binalshibh, Atta complained that some of the hijackers wanted to contact their families to say goodbye, something he had forbidden. Atta, moreover, was nervous about his future communications with Binalshibh, whom he instructed to obtain new telephones upon returning to Germany. Before Binalshibh left Spain, he gave Atta eight necklaces and eight bracelets that Atta had asked him to buy when he was recently in Bangkok, believing that if the hijackers were clean shaven and well dressed, others would think them wealthy Saudis and give them less notice.<sup>150</sup>

As directed, upon returning from Spain, Binalshibh obtained two new phones, one to communicate with Atta and another to communicate with KSM and others, such as Zacarias Moussaoui. Binalshibh soon contacted KSM and, using code words, reported the results of his meeting with Atta. This important exchange occurred in mid-July.<sup>151</sup>

The conversation covered various topics. For example, Jarrah was to send Binalshibh certain personal materials from the hijackers, including copies of their



passports, which Binalshibh in turn would pass along to KSM, probably for subsequent use in al Qaeda propaganda.<sup>152</sup>

The most significant part of the mid-July conversation concerned Jarrah's troubled relationship with Atta. KSM and Binalshibh both acknowledge that Jarrah chafed under Atta's authority over him. Binalshibh believes the disagreement arose in part from Jarrah's family visits. Moreover, Jarrah had been on his own for most of his time in the United States because Binalshibh's visa difficulty had prevented the two of them from training together. Jarrah thus felt excluded from the decisionmaking. Binalshibh had to act as a broker between Jarrah and Atta.<sup>153</sup>

Concerned that Jarrah might withdraw from the operation at this late stage, KSM emphasized the importance of Atta and Jarrah's resolving their differences. Binalshibh claims that such concern was unwarranted, and in their mid-July discussion reassured KSM that Atta and Jarrah would reconcile and be ready to move forward in about a month, after Jarrah visited his family. Noting his concern and the potential for delay, KSM at one point instructed Binalshibh to send "the skirts" to "Sally"—a coded instruction to Binalshibh to send funds to Zacarias Moussaoui. While Binalshibh admits KSM did direct him to send Moussaoui money during the mid-July conversation, he denies knowing exactly why he received this instruction—though he thought the money was being provided "within the framework" of the 9/11 operation.<sup>154</sup>

KSM may have instructed Binalshibh to send money to Moussaoui in order to help prepare Moussaoui as a potential substitute pilot for Jarrah. On July 20, 2001, Aysel Senguen, Jarrah's girlfriend, purchased a one-way ticket for Jarrah from Miami to Dusseldorf. On Jarrah's previous four trips from the United States to see Senguen and his family in Lebanon, he had always traveled with a round-trip ticket. When Jarrah departed Miami on July 25, Atta appears to have driven him to the airport, another unique circumstance.<sup>155</sup>

Binalshibh picked up Jarrah at the airport in Dusseldorf on July 25. Jarrah wanted to see Senguen as soon as possible, so he and Binalshibh arranged to meet a few days later. When they did, they had an emotional conversation during which Binalshibh encouraged Jarrah to see the plan through.<sup>156</sup>

While Jarrah was in Germany, Binalshibh and Moussaoui were in contact to arrange for the transfer of funds. Binalshibh received two wire transfers from Hawsawi in the UAE totaling \$15,000 and, within days, relayed almost all of this money to Moussaoui in two installments.<sup>157</sup>

Moussaoui had been taking flight lessons at the Airman Flight School in Norman, Oklahoma, since February but stopped in late May. Although at that point he had only about 50 hours of flight time and no solo flights to his credit, Moussaoui began making inquiries about flight materials and simulator training for Boeing 747s. On July 10, he put down a \$1,500 deposit for flight simulator training at Pan Am International Flight Academy in Eagan, Minnesota, and by the end of the month, he had received a simulator schedule to train from

August 13 through August 20. Moussaoui also purchased two knives and inquired of two manufacturers of GPS equipment whether their products could be converted for aeronautical use—activities that closely resembled those of the 9/11 hijackers during their final preparations for the attacks.<sup>158</sup>

On August 10, shortly after getting the money from Binalshibh, Moussaoui left Oklahoma with a friend and drove to Minnesota. Three days later, Moussaoui paid the \$6,800 balance owed for his flight simulator training at Pan Am in cash and began his training. His conduct, however, raised the suspicions of his flight instructor. It was unusual for a student with so little training to be learning to fly large jets without any intention of obtaining a pilot's license or other goal. On August 16, once the instructor reported his suspicion to the authorities, Moussaoui was arrested by the INS on immigration charges.<sup>159</sup>

KSM denies ever considering Moussaoui for the planes operation. Instead he claims that Moussaoui was slated to participate in a "second wave" of attacks. KSM also states that Moussaoui had no contact with Atta, and we are unaware of evidence contradicting this assertion.<sup>160</sup>

Yet KSM has also stated that by the summer of 2001, he was too busy with the planes operation to continue planning for any second-wave attacks. Moreover, he admits that only three potential pilots were ever recruited for the alleged second wave, Moussaoui plus two others who, by midsummer of 2001, had backed out of the plot.<sup>161</sup> We therefore believe that the effort to push Moussaoui forward in August 2001 lends credence to the suspicion that he was being primed as a possible pilot in the immediate planes operation.

Binalshibh says he assumed Moussaoui was to take his place as another pilot in the 9/11 operation. Recounting a post-9/11 discussion with KSM in Kandahar, Binalshibh claims KSM mentioned Moussaoui as being part of the 9/11 operation. Although KSM never referred to Moussaoui by name, Binalshibh understood he was speaking of the operative to whom Binalshibh had wired money. Binalshibh says KSM did not approve of Moussaoui but believes KSM did not remove him from the operation only because Moussaoui had been selected and assigned by Bin Ladin himself.<sup>162</sup>

KSM did not hear about Moussaoui's arrest until after September 11. According to Binalshibh, had Bin Ladin and KSM learned prior to 9/11 that Moussaoui had been detained, they might have canceled the operation. When Binalshibh discussed Moussaoui's arrest with KSM after September 11, KSM congratulated himself on not having Moussaoui contact the other operatives, which would have compromised the operation. Moussaoui had been in contact with Binalshibh, of course, but this was not discovered until after 9/11.<sup>163</sup>

As it turned out, Moussaoui was not needed to replace Jarrah. By the time Moussaoui was arrested in mid-August, Jarrah had returned to the United States from his final trip to Germany, his disagreement with Atta apparently resolved. The operatives began their final preparations for the attacks.<sup>164</sup>

### **Readying the Attacks**

A week after he returned from meeting Binalshibh in Spain, Atta traveled to Newark, probably to coordinate with Hazmi and give him additional funds. Atta spent a few days in the area before returning to Florida on July 30. The month of August was busy, as revealed by a set of contemporaneous Atta-Binalshibh communications that were recovered after September 11.<sup>165</sup>

On August 3, for example, Atta and Binalshibh discussed several matters, such as the best way for the operatives to purchase plane tickets and the assignment of muscle hijackers to individual teams. Atta and Binalshibh also revisited the question of whether to target the White House. They discussed targets in coded language, pretending to be students discussing various fields of study: “architecture” referred to the World Trade Center, “arts” the Pentagon, “law” the Capitol, and “politics” the White House.<sup>166</sup>

Binalshibh reminded Atta that Bin Ladin wanted to target the White House. Atta again cautioned that this would be difficult. When Binalshibh persisted, Atta agreed to include the White House but suggested they keep the Capitol as an alternate target in case the White House proved too difficult. Atta also suggested that the attacks would not happen until after the first week in September, when Congress reconvened.<sup>167</sup>









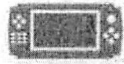





Atta and Binalshibh also discussed “the friend who is coming as a tourist”—a cryptic reference to candidate hijacker Mohamed al Kahtani (mentioned above), whom Hawsawi was sending the next day as “the last one” to “complete the group.” On August 4, Atta drove to the Orlando airport to meet Kahtani. Upon arrival, however, Kahtani was denied entry by immigration officials because he had a one-way ticket and little money, could not speak English, and could not adequately explain what he intended to do in the United States. He was sent back to Dubai. Hawsawi contacted KSM, who told him to help Kahtani return to Pakistan.<sup>168</sup>


On August 7, Atta flew from Fort Lauderdale to Newark, probably to coordinate with Hazmi. Two days later, Ahmed al Ghamdi and Abdul Aziz al Omari, who had been living in New Jersey with Hazmi and Hanjour, flew to Miami—probably signifying that the four hijacking teams had finally been assigned. While Atta was in New Jersey, he, Hazmi, and Hanjour all purchased tickets for another set of surveillance flights. Like Shehhi, Jarrah, Atta, and Waleed al Shehri before them, Hazmi and Hanjour each flew in first class on the same type of aircraft they would hijack on 9/11 (a Boeing 757), and on transcontinental flights that connected to Las Vegas. This time, however, Atta himself also flew directly to Las Vegas, where all three stayed on August 13–14. Beyond Las Vegas’s reputation for welcoming tourists, we have seen no credible evidence explaining why, on this occasion and others, the operatives flew to or met in Las Vegas.<sup>169</sup>

Through August, the hijackers kept busy with their gym training and the pilots took frequent practice flights on small rented aircraft. The operatives also

**Appendix B:** Hemispheres Magazine, August 2012 at 129.

**CUSTOMER CARE** We are committed to providing quality service, and we want to hear about your travel experience with us. In addition, if you think a certain employee or an action taken on your behalf deserves special recognition, please let us know. Please give us your feedback at [ualsurvey.com](http://ualsurvey.com).

ELECTRONIC DEVICES	
STAGE OF FLIGHT	DEVICES PERMITTED
<p><b>DEPARTURE:</b> at gate, only when cabin door is open</p> <p><b>ARRIVAL:</b> taxiing to gate area</p>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <p>Mobile phones and two-way pagers</p> </div> <div style="text-align: center;">  <p>PDA's and other electronic devices</p> </div> </div> <p style="text-align: center;"><b>MUST BE TURNED OFF:</b> during taxi, takeoff and landing</p>
<p><b>IN FLIGHT:</b> above 10,000 feet in altitude</p> <p><b>ON GROUND:</b> when main cabin door is open</p>	<div style="display: flex; justify-content: space-between;"> <div style="width: 15%;">  <p>Noise-canceling headphones</p> </div> <div style="width: 15%;">  <p>GPS devices</p> </div> <div style="width: 15%;">  <p>Entertainment players and recorders (audio and/or video, such as iPods; e-readers; tape/CD/MiniDisc/MP3/DVD players; and camcorders)*</p> </div> <div style="width: 15%;">  <p>Calculators</p> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 15%;">  <p>Cameras</p> </div> <div style="width: 15%;">  <p>Personal computers*</p> </div> <div style="width: 15%;">  <p>Electronic games*</p> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 15%;">  <p>Shavers</p> </div> <div style="width: 15%;">  <p>Aircraft power ports for laptops</p> </div> <div style="width: 15%;"> <p style="text-align: center;">* must be used with sound off or with headsets at all times</p> </div> </div> <p style="text-align: center;"><b>MUST BE TURNED OFF:</b> during taxi, takeoff and landing</p>
<p><b>NEVER PERMITTED</b></p>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <p>TVs</p> </div> <div style="text-align: center;">  <p>Radio receivers and/or transmitters (including AM/FM/SW, CB and scanners)</p> </div> <div style="text-align: center;">  <p>Remote-control toys and personal air purifiers</p> </div> </div>

 Rechargeable batteries have a risk of overload or fire when not stored properly. Rechargeable batteries should be stored in their electronic devices or properly protected to avoid contact with metal or other batteries during flight.

Advanced mobile phones, PDA's and other personal electronic devices with wireless capabilities may be used in flight when switched to "airplane" mode. A visible airplane-disabled mode should be identifiable and shown to a crew member upon request. Flight attendants will notify mobile phone and two-way pager users when it is safe to begin placing or receiving phone calls or pages after landing. One-way pagers may be used to receive messages at any time.

**PLEASE NOTE** Customers may always use any medically prescribed physiological instrument, such as a hearing aid or a pacemaker. On aircraft equipped with in-ear headphones, customers with hearing-assistance devices may request a different headset from a flight attendant.

Passengers are allowed to use non-battery-operated headphones during taxi, takeoff and landing.

The in-seat power system may be used only above 10,000 feet, when other approved personal electronic devices are permitted. Use of the system is at your own risk. Do not remove batteries. We are not responsible for loss of data or damage to computer hardware or software.

**ONBOARD PHOTO AND VIDEO** The use of still and video cameras, film or digital, including any cellular or other devices that have this capability, is permitted only for recording of personal events. Photography or audio or video recording of other customers without their express prior consent is strictly prohibited. Also, unauthorized photography or audio or video recording of airline personnel, aircraft equipment or procedures is always prohibited. Any photography (video or still) or voice or audio recording or transmission while on any United Airlines aircraft is strictly prohibited, except to the extent specifically permitted by United Airlines.

**PLEASE NOTE** United strictly prohibits the modification or use of any object or device to alter or limit the functionality, permanently or temporarily, of any aircraft structure, seat assembly, tray table, etc. If you see a customer using any such device or object, please inform United personnel immediately.

**Appendix C:** American Way (April 1, 2013), p. 80.



# THE NATIONAL PASTIME

CARD-CARRYING EXPERT | THE DH TURNS 40 | HARRISON FORD ► PLAYS A DODGERS LEGEND | NEIGHBORHOOD BALLPARKS



APRIL 01, 2013

# AMERICAN WAY

AMERICAN AIRLINES + AMERICAN EAGLE

TWO OF TWO  
COLLECTIBLE COVERS



# Triple Threat

The Detroit Tigers' **MIGUEL CABRERA** looks to top his Triple Crown with a World Series championship

WIDE WORLD

# Onboard Our Flights



American Airlines supports FAA efforts to keep passengers and crew safe when traveling.

## What's in Your Baggage?

Common items used every day may seem harmless. However, when transported by air, they can become dangerous. During flight, variations in pressure and temperature can cause items to leak, generate toxic fumes or ignite.

**The list of items prohibited by the FAA includes:** aerosols, pepper spray/Mace, fireworks, black powder, model-rocket motors, explosive primers, strike-anywhere matches, fuels, camping gas, lighter refills, paints, solvents, alcohols, nail polishes/removers over half an ounce, bleaches, drain cleaners, acids, lead-acid batteries, flares, gas-powered tools and self-heating meals. Such items are confiscated by the TSA and reported to the FAA.

**Lithium and lithium-ion batteries** catch fire when improperly handled and are prohibited in checked baggage. They're allowed in carry-on baggage only, not exceeding 160 watt-hours each (limit two over 100wh). [Safetravel.dot.gov](http://safetravel.dot.gov) provides battery-size guidance. Carry batteries in original packaging, in separate plastic bags or with electrical tape on contacts. **Do not use aircraft powerports to charge batteries when not in use.**

**Carrying prohibited items on aircraft violates U.S. federal law.** Violators are subject to imprisonment and penalties of \$250,000 or more. For more information, consult an agent or visit [Safetravel.dot.gov](http://Safetravel.dot.gov) or [aa.com](http://aa.com).

## Things You Need to Know to Make Your Trip Safe and Comfortable

■ **Check-In** We advise customers to check in 90 minutes before their scheduled departure for domestic flights when checking bags, 60 minutes with no bags and two hours for international flights. (Please refer to the Travel Information section on [aa.com](http://aa.com) for cities where earlier check-in is recommended.) This will help ensure your reservation and seat assignment. Please be onboard and in your seat with your seat belt fastened 10 minutes prior to departure time.

■ **Luggage** For domestic economy-class tickets (including to and from Puerto Rico and the U.S. Virgin Islands) purchased on or after Feb. 1, 2010, a \$25 charge applies for the first checked bag and a \$35 charge applies for the second checked bag. The same charges apply for economy-class tickets between the United States/Puerto Rico/U.S. Virgin Islands and Canada purchased on or after March 29, 2010. For economy-class tickets between the United States/Puerto Rico/U.S. Virgin Islands and Europe or India purchased on or after Sept. 14, 2009, the first bag may be checked at no charge and a \$50 charge applies for the second checked bag. For economy-class tickets between the United States/Puerto Rico/U.S. Virgin Islands, Europe or India and Mexico purchased on or after May 3, 2010, the first bag may be checked at no charge and a \$30 charge applies for the second checked bag (exceptions apply for all baggage charges). Passengers may carry one piece of luggage and one personal item onboard. Carry-on items, including laptop computers, must be placed in the overhead bin or under the seat in front of you. To avoid additional charges, all luggage must meet size and weight requirements. Liability for loss, delay or damage to baggage is limited, so carry valuables onboard with you. Visit [aa.com/baggage](http://aa.com/baggage) for more.

■ **Beverage Service** Only alcohol served by a flight attendant to

customers age 21 or older may be consumed onboard. By FAA rule, we may not serve alcohol to customers who appear intoxicated.

■ **Smoking** is not permitted. Also, smokeless/e-cigarettes may not be used at any time while onboard.

■ **Seat Belts** Turbulence is air movement that cannot be seen and that often occurs unexpectedly. While we do everything possible to avoid turbulence, it is the most likely threat to your in-flight safety. Unless you must leave your seat, keep your seat belt fastened at all times, even when the seat-belt sign is off.

■ **Disability Assistance** Customers who need assistance with disabilities, including obtaining wheelchairs, should contact an American representative. Per government regulations, service animals traveling in the cabin to assist passengers with physical or emotional needs are not required to travel in a kennel. If you are in a bulkhead seat, you may be asked to move to another seat to accommodate a service animal. To give feedback on how well American provided disability-related services, call (817) 967-3000.

■ **Carry-on Pets** must stay in their closed and/or zipped kennels and under the seat in front of you at all times. American assumes no liability for the well-being of carry-on pets.

■ **Powerports** On most aircraft, there is a DC cigarette-lighter-style outlet at each seat in First and Business Class and in select rows in the Main Cabin for powering approved electronic devices. For information about powerports, visit [aa.com](http://aa.com). New B737 aircraft offer 110V AC power outlets in every row. Only one device per outlet is allowed.

**Federal law prohibits passengers from threatening or intimidating the flight crew or interfering as crew members perform their duties.**

■ **Electronic Equipment/Personal Devices** Personal electronic devices may be used during boarding until the flight attendant's announcement to switch them off. After the announcement, all portable electronic devices must remain off and properly stored (electronic devices include but are not limited to e-books). During this period, noise-canceling headsets may be worn while switched off and devices without power switches (e.g., some PDAs) must be stored and remain in the sleep mode. During flight, your flight attendant will inform you when approved devices may be used. Cellular PDAs (provided they are in airplane/flight mode) are permitted. Audio and video equipment may be used only with headsets, and noise-canceling headsets may be activated. The use of still and video cameras, film or digital, is permitted only for recording of personal events. Unauthorized photography or video recording of airline personnel, other customers, aircraft equipment or procedures is strictly prohibited. Never activate two-way pagers, radios, TV sets, remote controls, cordless computer mice or commercial TV cameras. All devices with transmitting capabilities must be switched off except Wi-Fi 802.11. Wi-Fi 802.11 devices may be used (when authorized) only on aircraft equipped with in-flight Internet service. If in-flight Internet service is provided, it is intended for customer access to the Internet, email and VPN only. Any voice, audio, video or other photography (motion or still), recording or transmission while on any American aircraft is strictly prohibited, except to the extent specifically permitted by American Airlines. Before landing, your flight attendant will announce when to switch off and store all electronic devices. These devices must remain off until the plane is at the gate and the seat-belt sign has been switched off.

The electronic-device policy may vary on American Eagle and AmericanConnection. Please see a flight attendant for specifics.



**Appendix D: Dictionary pages**

We use cookies to enhance your experience on our website. By continuing to use our website, you are agreeing to our use of cookies. You can change your cookie settings at any time. [Continue](#) or [Find out more](#) X

[Help](#) [Log in](#) or [Subscribe](#)

[Dictionary](#) [Better writing](#) [World of words](#) [Puzzles and games](#) [For children and schools](#) [For learners of English](#)

[Dictionary](#) [Language resources](#)


[British & World English](#) 

**Only  
Brainwashing  
is Faster**

Scientific discovery reveals how you can start speaking a language in just 10 days using this sneaky linguistic secret. This method was recommended by Forbes and purchased by the FBI.

[Click here  
for full story](#)



**Pimsleur Approach**

AIR CANADA

**LOWEST PRICE  
GUARANTEE**

Always at [aircanada.com](http://aircanada.com)

**STOP SEARCHING FAR AND WIDE.**

**> BOOK NOW**

[aircanada.com](http://aircanada.com)

# term

| [Cite](#)

Pronunciation: [/tɜːm/](#)

Translate **term** | [into French](#) | [into German](#) | [into Italian](#) | [into Spanish](#)

## Definition of **term**

### *noun*

**1** a word or phrase used to describe a thing or to express a concept, especially in a particular kind of language or branch of study:

*the musical term 'leitmotiv'*

*a term of abuse*

- (**terms**) language used on a particular occasion; a way of expressing oneself:

*a protest in the strongest possible terms*

- *Logic* a word or words that may be the subject or predicate of a proposition.

**2** a fixed or limited period for which something, for example office, imprisonment, or investment, lasts or is intended to last:

*the President is elected for a single four-year term*

- (also **term day**) (especially in Scotland) a fixed day of the year appointed for the making of payments, the start or end of tenancies, etc..
- (also **full term**) [*mass noun*] the completion of a normal length of pregnancy: *the pregnancy went to full term*
- (*British* also **term of years** or *US term for years*) *Law* a tenancy of a fixed period.
- *archaic* the duration of a person's life.
- *archaic* a boundary or limit, especially of time.

**3** each of the periods in the year, alternating with holiday or vacation, during which instruction is given in a school, college, or university, or during which a law court holds sessions:

*the summer term*

*term starts tomorrow*

**4** (**terms**) conditions under which an action may be undertaken or agreement reached; stipulated or agreed requirements:

## More results for **term**

[full term](#) Br. Eng

[half-term](#) Br. Eng

[law term](#) Br. Eng

[Lent term](#) Br. Eng

[long-term](#) Br. Eng

[near-term](#) Br. Eng

[Result list for \*\*term\*\*](#)

## More words in this category

[code-switching](#)

[cognitive grammar](#)

[collocation](#)

[concordance](#)

[definiens](#)

[dialectology](#)

[encyclopedic](#)

[endophora](#)

[grave](#)<sup>2</sup>

[hypocoristic](#)

[idiom](#)

[minimal](#)

[mixed metaphor](#)

[onomastic](#)

[pidgin](#)

[prosthesis](#)

[Saussure, Ferdinand de](#)

[semasiology](#)

[semiosis](#)

[univocal](#)

## Word of the day

[orison](#)

*their solicitors had agreed terms*

*he could only be dealt with **on his own terms***

- conditions with regard to payment for something; stated charges:  
*loans on favourable terms*
- agreed conditions under which a war or other dispute is brought to an end:

*the United States played a key role in prodding the two sides to **come to terms***

**5 Mathematics** each of the quantities in a ratio, series, or mathematical expression.

**6 Architecture** another term for TERMINUS.

*verb*

[with object and usually with complement]

give a descriptive name to; call by a specified term:

*he has been termed the father of modern theology*

### Phrases

#### come to terms with

come to accept (a new and painful or difficult event or situation); reconcile oneself to:

*she had come to terms with the tragedies in her life*

#### in terms of (or in — terms)

with regard to the particular aspect or subject specified:

*replacing the printers is difficult to justify in terms of cost*

#### the long/short/medium term

used to refer to a time that is a specified way into the future:

*these ventures are unlikely to yield much return **in the short term***

#### on terms

in a state of friendship or equality.

(in sport) level in score or on points.

#### on — terms

in a specified relation or on a specified footing:

*we are all on friendly terms*

#### terms of reference

see REFERENCE.

#### Origin:

Middle English (denoting a limit in space or time, or (in the plural) limiting conditions): from Old French *terme*, from Latin *terminus* 'end, boundary, limit'

**term** in other Oxford dictionaries

Definition of **term** in the [US English](#) dictionary

## Reference to **term** in Language Resources

- [Is there a term for the study of love?](#)

/ ˈtɜːm(ə)n /

noun




a prayer ...

[See full definition »](#)

**SIGN UP**

- What is the origin of the term 'UFO'?
- What is the origin of the term 'brass monkey'?
- What is the origin of the term 'flea market'?
- What is the collective term for a group of cats?
- What is the origin of the term 'dressed to the nines'?

**Seize Today's Top Bargains**

		
Swimways Spring Float	Swimways Spring Float	Swimways Pool Spring
<b>\$25.88*</b>	<b>\$26.66*</b>	<b>\$19.57*</b>
1 seller	6 sellers	8 sellers

**Nextag** © 2011, Nextag, Inc. \*Price and availability subject to change.

## Nearby words

- tergum
- Terhune, Albert Payson
- -teria
- teriyaki
- Terkel, Studs
- **term**
- term life insurance
- term paper
- term time
- termagant
- terminable

Type a word or phrase

Go

British & World English

Seize Today's Top Bargains!  
Nextag  
\*Price and availability subject to change.



Wolf Sunglass Neck Strap  
\$9.49\*  
Compare Prices



GoodyBeads Eyeglass holder  
\$5.99\*  
Compare Prices



Bauble LuLu Bead 28"  
\$14.95\*  
Compare Prices

© 2012, Nextag, Inc.

"Could I be doing better financially?"

Drag across to change.

# condition

| Cite

Pronunciation: /kənˈdɪʃ(ə)n/

Translate **condition** | into French | into German | into Italian | into Spanish

## Definition of **condition**

*noun*

**1** [*mass noun, usually with adjective*] the state of something with regard to its appearance, quality, or working order:

*the wiring is in good condition*

[*in singular*]:

*the bridge is in an extremely dangerous condition*

- a person's or animal's state of health or physical fitness:  
*the baby was in good condition at birth*

[*in singular*]:

*she was in a serious condition*

- [*count noun, often with modifier*] an illness or other medical problem:  
*a heart condition*

- [*in singular*] the situation in life of a particular group:  
*the sorrows of the human condition*

- *archaic* social position:  
*those of humbler condition*

**2 (conditions)** the circumstances or factors affecting the way in which people live or work, especially with regard to their well-being:

*harsh working and living conditions*

- the factors or prevailing situation influencing the performance or outcome of a process:  
*present market conditions*

- the prevailing state of the weather, ground, or sea at a particular time, especially as it affects a sporting event:  
*the appalling conditions determined the style of play*

**3** a situation that must exist before something else is possible or permitted:

*for a member to borrow money, three conditions have to be met*

*all personnel should comply with this policy as **a condition of** employment*

## More results for **condition**

[condition code](#) Br. Eng

[truth condition](#) Br. Eng

[boundary condition](#) Br. Eng

[in mint condition](#) *in mint*<sup>2</sup> Br. Eng

[preexisting condition](#) Br. Eng

[in a delicate condition](#) *in delicate* Br. Eng

Result list for **condition**

## Word of the day

**orison**

/ ˈɒrɪz(ə)n /

*noun*

a prayer ...

[See full definition »](#)

**SIGN UP**

*verb*

[*with object*]

**1** have a significant influence on or determine (the manner or outcome of something):

*national choices are conditioned by the international political economy*

- train or accustom to behave in a certain way or to accept certain circumstances:

*our minds are heavily conditioned and circumscribed by habit*

[*with object and infinitive*]:

*they are beliefs which he has been conditioned to accept*

(as noun **conditioning**)

*social conditioning*

**2** bring (something) into the desired state for use:

*a product for conditioning leather*

- (often as adjective **conditioned**) make (a person or animal) fit and healthy:

*he was six feet two of perfectly conditioned muscle and bone*

- (often as adjective **conditioned**) bring (beer) to maturation after fermentation while the yeast is still present:

[*in combination*]:

*cask-conditioned real ales*

- [*no object*] (of a beer) become conditioned:

*brews that are allowed to condition in the bottle*

**3** apply a conditioner to (the hair):

*I condition my hair regularly*

**4** set prior requirements on (something) before it can occur or be done:

*Congressmen have sought to limit and condition military and economic aid*

### Phrases

#### in (or out of) condition

in a fit (or unfit) physical state:

*what difference should it make to the coach what I do after hours as long as I keep in condition?*

*'I'm out of condition,' she panted*

#### in no condition to do something

certainly not fit or well enough to do something:

*you're in no condition to tackle the stairs*

#### on condition that

with the stipulation that:

*I got three years' probation, on condition that I stay at the hostel for a year*

### Origin:

Middle English: from Old French *condicion* (noun), *condicionner* (verb), from Latin *condicio(n)-* 'agreement', from *condicere* 'agree upon', from *con-* 'with' + *dicere* 'say'

## Grammar

When writing or speaking we often wish to show that one event depends on another in some way:

*If the weather was fine, Maud liked to walk in Hyde Park.*

One statement, *Maud liked to walk in Hyde Park*, is **conditional** upon the other *the weather was fine*. Conditional clauses are usually introduced by either *if* or *unless*. They can express a number of different meanings. Common events They can state general truths, such as:

***If water penetrates window sills, doors, or their frames, the result is wet rot.***

In sentences like this the verb is in the present tense. It is also possible to use the past tense to describe general truths about the past:

***If the weather was fine, Maud liked to walk in Hyde Park.***

Possible events Conditional clauses can describe situations which have not yet happened, but are possible:

***If it comes to court, you two can testify.***

Here both verbs are in the present tense. Similar sentences can be constructed using *unless*:

***Policemen don't find bodies unless they are sent to look for them or unless someone else has found them first.***

Here *unless* has the meaning of *if...not...*:

***Policemen don't find bodies if they aren't sent to look for them or if someone else hasn't found them first.***

Future events Very often conditional clauses speculate about events in the future. Such clauses can be open or closed. In an open conditional the speaker expresses no opinion about whether the future event is likely to happen or not:

***If they succeed in that, Germany's economy and its workers will be better off.***

(The writer has no opinion of whether they will succeed or not.) In a closed condition the writer makes it clear that the future event is more or less unlikely:

***If they were successful at this stage, they would then have to find the fee.***

(But they are not likely to be successful.) Past events Conditional clauses can also be used to speculate about how things might have turned out in the past:

***If they had been her own children, she would have used them differently.***

But they weren't her own children, so she treated them as she did. The condition cannot be fulfilled because it is impossible. Clauses that are not introduced by a conjunction It is possible to construct conditional clauses that do not begin with *if* or *unless*. The commonest way of doing this is to begin the clause with one of these words:

*were should had*

For example:

***Were I to own a new BMW car, another ten microcomputers would be at my command, so their advertisements claim. Should you succeed in becoming a planner, you would be helping to create these parameters.***

***Had I been in a vehicle, I could have gone back, but on foot it was not worth risking the wasted energy.***

**condition** in other Oxford dictionaries

Definition of **condition** in the [US English](#) dictionary

## Reference to **condition** in Language Resources

- [Phrase, Fable, and Allusion](#)



### Nearby words

- [condescend](#)
- [condescending](#)
- [condescension](#)
- [condign](#)
- [condiment](#)
- **condition**
- [condition code](#)
- [conditional](#)
- [conditional discharge](#)
- [conditional probability](#)
- [conditional sale](#)

Copyright © 2013 Oxford University Press. All rights reserved | [Privacy policy and legal notice](#) | [Credits](#) | [Browse dictionary](#) | [About](#) | [Subscriber services](#) | [What's new](#) | [Contact us](#)  
[British & World version](#) | [US Version](#) | [Versión en español](#)



# Black's Law Dictionary®

**Eighth Edition**

**Bryan A. Garner**  
Editor in Chief

**THOMSON**  
—★—™  
**WEST**

Mat #40231642  
Mat #40235008—deluxe

action for the recovery of a specified quantity of a named commodity.

**conditio** (kən-dish-ee-oh). [Latin] A condition.

**conditio sine qua non.** See SINE QUA NON.

**conditio si sine liberis decesserit** (kən-dish-ee-oh si sine lib-ər-is di-ses-ər-it). [Latin "the condition if he should have died childless"] *Roman law.* An express or implied clause in a will providing that if the heir or legatee dies childless, the property is to go to another person, such as the testator's own descendants.

**condition, n. 1.** A future and uncertain event on which the existence or extent of an obligation or liability depends; an uncertain act or event that triggers or negates a duty to render a promised performance. • For example, if Jones promises to pay Smith \$500 for repairing a car, Smith's failure to repair the car (an implied or constructive condition) relieves Jones of the promise to pay. [Cases: Contracts § 218-227. C.J.S. *Architects* § 16; *Contracts* §§ 355-358, 362, 444-445, 450, 557-560.]

"'Condition' is used in this Restatement to denote an event which qualifies a duty under a contract. It is recognized that 'condition' is used with a wide variety of other meanings in legal discourse. Sometimes it is used to denote an event that limits or qualifies a transfer of property. In the law of trusts, for example, it is used to denote an event such as the death of the settlor that qualifies his disposition of property in trust. Sometimes it is used to refer to a term in an agreement that makes an event a condition, or more broadly to refer to any term in an agreement (e.g., 'standard conditions of sale'). For the sake of precision, 'condition' is not used here in these other senses." *Restatement (Second) of Contracts* § 224 cmt. a (1981).

"Strictly, a condition is a fact or event on the occurrence of which some legal right or duty comes into existence; a party may promise that this fact is so, or that the event will take place, but it is equally possible that no party to the contract promises this. An insurance company promises to pay £10,000 to an insured person if his house is destroyed by fire; the destruction of the house by fire is a condition of the insurer's promise to pay, but neither party promises to burn the house." P.S. Atiyah, *An Introduction to the Law of Contract* 146 (3d ed. 1981).

"Promises and the duties they generate can be either unconditional ('I promise to pay you \$100,000') or conditional ('I promise to pay you \$100,000 if your house burns down'). Lawyers use *condition* in several senses. Sometimes they use it to refer to the term in the agreement that makes the promise conditional. . . . However, lawyers also use *condition* to refer to an operative fact rather than to a term. According to the Restatement Second a condition is 'an event, not certain to occur, which must occur, unless occurrence is excused, before performance under a contract becomes due.' This use of the word has the support of leading writers." E. Allan Farnsworth, *Contracts* § 8.2, at 519-20 (3d ed. 1999).

**2.** A stipulation or prerequisite in a contract, will, or other instrument, constituting the essence of the instrument. • If a court construes a contractual term to be a condition, then its untruth or breach will entitle the party to whom it is made to be discharged from all liabilities under the contract. [Cases: Contracts § 218-227; Wills § 639-668. C.J.S. *Architects* § 16; *Contracts* §§ 355-358, 362, 444-445, 450, 557-560; *Wills* §§ 1380-1424.]

**affirmative condition.** See *positive condition.*

**casual condition.** *Civil law.* A condition that depends on chance; one that is not within the power of either party to an agreement.

**collateral condition.** A condition that requires the performance of an act having no relation to an agreement's main purpose.

**compulsory condition.** A condition expressly requiring that a thing be done, such as a tenant's paying rent on a certain day.

**concurrent condition.** A condition that must occur or be performed at the same time as another condition, the performance by each party separately operating as a condition precedent; a condition that is mutually dependent on another, arising when the parties to a contract agree to exchange performances simultaneously. — Also termed *condition concurrent.* [Cases: Contracts § 225. C.J.S. *Contracts* § 362.]

"'Conditions concurrent' are acts that the parties to a contract are under duties of performing concurrently, the act of each party being separately operative as a condition precedent. The act is not concurrent with the legal relation affected, but only with the act of the other party." William R. Anson, *Principles of the Law of Contract* 412-13 (Arthur L. Corbin ed., 3d Am. ed. 1919).

**condition implied by law.** See *constructive condition.*

**condition implied in law.** See *constructive condition.*

**condition precedent** (pɹə sɛd-ənt also pres-ə-dənt). An act or event, other than a lapse of time, that must exist or occur before a duty to perform something promised arises. • If the condition does not occur and is not excused, the promised performance need not be rendered. The most common condition contemplated by this phrase is the immediate or unconditional duty of performance by a promisor. [Cases: Contracts § 221. C.J.S. *Contracts* §§ 356, 444-445, 450.]

"Before one gets too confused by the precedent and subsequent classifications, it might be helpful to know that in contract law there is no substantive difference between the two. . . . However, in the area of pleading and procedure significance may be placed upon the difference between a condition precedent and subsequent in terms of who has the burden of pleading and proof, the party seeking to enforce the promise usually being required to plead and prove a condition precedent and the party seeking to avoid liability for breach of promise sometimes being required to plead and prove the occurrence of the condition subsequent that would terminate his duty." Claude Rohwer & Gordon D. Schaber, *Contracts in a Nutshell* 313 (4th ed. 1997).

**condition subsequent.** A condition that, if it occurs, will bring something else to an end; an event the existence of which, by agreement of the parties, discharges a duty of performance that has arisen. [Cases: Contracts § 226. C.J.S. *Architects* § 16; *Contracts* § 357.]

"If . . . the deed or will uses such words as 'but if,' 'on condition that,' 'provided, however,' or 'if, however,' it will generally be assumed that a condition subsequent was intended." Thomas F. Bergin & Paul G. Haskell, *Preface to Estates in Land and Future Interests* 50 (2d ed. 1984).

**constructive condition.** A condition contained in an essential contractual term that, though omitted by the parties from their agreement, a court has supplied as being reasonable in the circumstances; a condition imposed by law to do justice. • The cooperation of the parties to a contract, for example, is a constructive condition. — Also termed *implied-in-law condition*; *condition implied by law*; *con-*

*dition implied in law.* Cf. *implied-in-fact condition.* [Cases: Contracts  $\S$ 220. C.J.S. *Contracts*  $\S$  355.]

"[C]onstructive conditions are imposed by law to do justice. . . . The dividing line between an express condition and constructive conditions is often quite indistinct. Yet, the distinction is often of crucial importance. The general rule governing an express condition is that it must be strictly performed. The general rule as to constructive conditions is that substantial compliance is sufficient." John D. Calamari & Joseph M. Perillo, *The Law of Contracts*  $\S$  11.8, at 402 (4th ed. 1998).

**copulative condition** (kop-yə-lə-tiv or -lay-tiv). A condition requiring the performance of more than one act. Cf. *disjunctive condition*; *single condition*.

**dependent condition.** A mutual covenant that goes to the consideration on both sides of a contract.

**disjunctive condition.** A condition requiring the performance of one of several acts. Cf. *copulative condition*; *single condition*.

**dissolving condition.** See *resolutive condition*.

**express condition.** 1. A condition that is the manifested intention of the parties. [Cases: Contracts  $\S$ 219.]

"[E]xpress conditions . . . are conditions created through the agreement of the parties. This is so whether the intention to have the duty subject to a condition be manifested in words, or through any other conduct or type of utterance." John Edward Murray Jr., *Murray on Contracts*  $\S$  143, at 290 (2d ed. 1974).

2. A condition that is explicitly stated in an instrument; esp., a contractual condition that the parties have reduced to writing.

**implied condition.** A condition that is not expressly mentioned, but is imputed by law from the nature of the transaction or the conduct of the parties to have been tacitly understood between them as a part of the agreement. See *constructive condition*; *implied-in-fact condition*. [Cases: Contracts  $\S$ 220. C.J.S. *Contracts*  $\S$  355.]

**implied-in-fact condition.** A contractual condition that the parties have implicitly agreed to by their conduct or by the nature of the transaction. Cf. *constructive condition*. [Cases: Contracts  $\S$ 220. C.J.S. *Contracts*  $\S$  355.]

**implied-in-law condition.** See *constructive condition*.

**inherent condition.** A condition that is an intrinsic part of an agreement; a condition that is not newly imposed but is already present in an agreement.

**lawful condition.** A condition that can be fulfilled without violating the law.

**mixed condition.** *Civil law.* A condition that depends either on the will of one party and the will of a third person, or on the will of one party and the happening of a causal event.

**negative condition.** A condition forbidding a party from doing a certain thing, such as prohibiting a tenant from subletting leased property; a promise not to do something, usu. as part of a larger agreement. — Also termed *restrictive condition*. See *negative easement* under EASEMENT.

**positive condition.** A condition that requires some act, such as paying rent. — Also termed *affirmative condition*.

**potestative condition** (poh-tes-tə-tiv). *Civil law.* A condition that will be fulfilled only if the obligated party chooses to do so. • Louisiana no longer uses this term, instead providing that this type of condition will render the obligation null. La. Civ. Code art. 1770. Cf. *suspensive condition*; *resolutive condition*. [Cases: Contracts  $\S$ 10. C.J.S. *Contracts*  $\S$  108.]

**preexisting condition.** *Insurance.* A physical or mental condition evident during the period before the effective date of a medical-insurance policy. • Typically, coverage for later treatment for such a condition is excluded if symptoms of the condition were present during the period before the policy was effective. [Cases: Insurance  $\S$ 2475.]

**promissory condition.** A condition that is also a promise.

"The distinction between a condition which is also a promise, and a condition which is not the subject of a promise, is often one of great difficulty and importance, especially where the term is implied and not expressed, and it is unfortunate that legal usage has sanctioned the word 'condition' for two such different concepts. It would at least be desirable if lawyers could be persuaded to refer to conditions which are the subject of a promise as 'promissory conditions', a usage which it is proposed to adopt here." P.S. Atiyah, *An Introduction to the Law of Contract* 147 (3d ed. 1981).

**resolutive condition** (rə-zol-yə-tor-ee). *Civil law.* A condition that upon fulfillment terminates an already enforceable obligation and entitles the parties to be restored to their original positions. — Also termed *resolutive condition*; *dissolving condition*. Cf. *potestative condition*.

**restrictive condition.** See *negative condition*.

**single condition.** A condition requiring the performance of a specified thing. Cf. *copulative condition*; *disjunctive condition*.

**suspensive condition.** *Civil law.* A condition that makes an obligation mandatory only if a specified but uncertain event occurs. Cf. *potestative condition*. [Cases: Contracts  $\S$ 222. C.J.S. *Contracts*  $\S\S$  356-357.]

**testamentary condition.** A condition that must be satisfied before a gift made in a will becomes effective.

**triggering condition.** A circumstance that must exist before a legal doctrine applies; esp., in criminal law, a circumstance that must exist before an actor will be entitled to a justification defense.

**unlawful condition.** A condition that cannot be fulfilled without violating the law.

3. Loosely, a term, provision, or clause in a contract. [Cases: Sales  $\S$ 85(1); Vendor and Purchaser  $\S$ 79. C.J.S. *Sales*  $\S\S$  99-101, 154; *Vendor and Purchaser*  $\S\S$  125, 141.]

"This term *condition* is generally used to describe any fact, subsequent to the formation of a contract, which operates to make the duty of a promisor immediately active and compelling. Such a fact may be described as such in a term of the contract or it may not. In either event, the *term* of the contract should not itself be called the *condition*. . . . It is not uncommon, popularly, to speak of a condition of the contract as synonymous with *term* or *provision* of the contract. This should be avoided." William R. Anson, *Principles*

of the Law of Contract 226 n.1 (Arthur L. Corbin ed., 3d Am. ed. 1919).

"The word 'condition' is used in the law of property as well as in the law of contract and it is sometimes used in a very loose sense as synonymous with 'term,' 'provision,' or 'clause.' In such a sense it performs no useful service." *Id.* at 409.

4. A qualification attached to the conveyance of property providing that if a particular event does or does not take place, the estate will be created, enlarged, defeated, or transferred. 5. A state of being; an essential quality or status. — **condition**, *vb.*

**artificial condition.** A physical characteristic of real property, brought about by a person's affirmative act instead of by natural forces.

**dangerous condition.** 1. A property defect creating a substantial risk of injury when the property is used in a reasonably foreseeable manner. • A dangerous condition may result in waiver of sovereign immunity. [Cases: Automobiles ☞258; Municipal Corporations ☞847; Negligence ☞1086. C.J.S. *Motor Vehicles* §§ 443, 448-449, 451, 463-464, 467; *Municipal Corporations* §§ 805-807; *Negligence* §§ 469-470, 573-574, 580.] 2. A property risk that children, because of their immaturity, cannot appreciate or avoid. [Cases: *Negligence* ☞1016, 1067. C.J.S. *Negligence* §§ 472-495, 513.]

**conditional, adj.** Subject to or dependent on a condition <a conditional sale>.

**conditional acceptance.** See ACCEPTANCE (4).

**conditional adjournment.** See ADJOURNMENT.

**conditional admissibility.** See ADMISSIBILITY.

**conditional assault.** See ASSAULT.

**conditional assignment.** See ASSIGNMENT (2).

**conditional bequest.** See BEQUEST.

**conditional contraband.** See CONTRABAND.

**conditional contract.** See CONTRACT.

**conditional conveyance.** See CONVEYANCE.

**conditional covenant.** See COVENANT (1).

**conditional creditor.** See CREDITOR.

**conditional delivery.** See DELIVERY.

**conditional devise.** See DEVISE.

**conditional divorce.** See *conversion divorce* under DIVORCE.

**conditional duty.** See DUTY (1).

**conditional estate.** See *estate on condition* under ESTATE (1).

**conditional fee.** 1. See *fee simple conditional* under FEE SIMPLE. 2. CONTINGENT FEE.

**conditional guaranty.** See GUARANTY.

**conditional indorsement.** See INDORSEMENT.

**conditional judgment.** See JUDGMENT.

**conditional legacy.** See LEGACY.

**conditional limitation.** See LIMITATION.

**conditionally privileged communication.** See COMMUNICATION.

**conditional obligation.** See OBLIGATION.

**conditional pardon.** See PARDON.

**conditional payment.** See PAYMENT.

**conditional plea.** See PLEA (1).

**conditional presumption.** See *rebuttable presumption* under PRESUMPTION.

**conditional privilege.** See *qualified privilege* under PRIVILEGE (1).

**conditional promise.** See PROMISE.

**conditional proof.** See PROOF.

**conditional purpose.** 1. An intention to do something, conditions permitting. 2. *Criminal law.* A possible defense against a crime if the conditions make committing the crime impossible (e.g., "I will steal the money if it's there," and the money is not there).

**conditional release.** See RELEASE.

**conditional revocation.** See DEPENDENT RELATIVE REVOCATION.

**conditional right.** See RIGHT.

**conditional sale.** See SALE.

**conditional sales contract.** See INSTALLMENT CONTRACT.

**conditional sentence.** See SENTENCE.

**conditional use.** See USE (1).

**conditional-use permit.** See SPECIAL-USE PERMIT.

**conditional will.** See WILL.

**conditional zoning.** See ZONING.

**condition concurrent.** See *concurrent condition* under CONDITION (2).

**condition implied by law.** See *constructive condition* under CONDITION (2).

**condition implied in law.** See *constructive condition* under CONDITION (2).

**conditioning the market.** See GUN-JUMPING.

**condition of employment.** A qualification or circumstance required for obtaining or keeping a job.

**condition precedent.** See CONDITION (2).

**conditions of sale.** The terms under which auctions are to be conducted. • The conditions of sale are usu. placed in the auction room for public viewing before the sale. [Cases: *Auctions and Auctioneers* ☞7. C.J.S. *Auctions and Auctioneers* §§ 2, 8.]

**condition subsequent.** See CONDITION (2).

**condominia** (kon-də-min-ee-ə). *Civil law.* Coownerships or limited ownerships. • *Condominia* are considered part of the *dominium* of the property, and thus are more than mere rights in the property (i.e., *jura in re aliena*); examples of *condominia* include *emphyteusis*, *superficies*, *pignus*, *hypotheca*, *usufructus*, *usus*, and *habitatio*.

**condominium** (kon-də-min-ee-əm). 1. Ownership in common with others. 2. A single real-estate unit in a multi-unit development in which a person has both

10-Q is less detailed than the 10-K. — Also termed *Form 10-Q*. [Cases: Securities Regulation Ⓒ60.27(6). C.J.S. *Securities Regulation* § 176.]

**tentative agenda.** See *proposed agenda* under AGENDA.

**tentative trust.** See *Totten trust* under TRUST.

**Tenth Amendment.** The constitutional amendment, ratified as part of the Bill of Rights in 1791, providing that any powers not constitutionally delegated to the federal government, nor prohibited to the states, are reserved for the states or the people. — Also termed *Reserved Power Clause*. [Cases: States Ⓒ4.16. C.J.S. *States* §§ 25–26.]

**1031 exchange (ten-thər-tee-wən).** An exchange of like-kind property that is exempt from income-tax consequences under IRC (26 USCA) § 1031. [Cases: Internal Revenue Ⓒ3184. C.J.S. *Internal Revenue* §§ 120–121, 124.]

**tenure (ten-yər), n.** 1. A right, term, or mode of holding lands or tenements in subordination to a superior. • In feudal times, real property was held predominantly as part of a tenure system. 2. A particular feudal mode of holding lands, such as socage, gavelkind, villeinage, and frankalmoign.

"Most of the feudal incidents and consequences of socage tenure were expressly abolished in New York by the act of 1787; and they were [later] wholly and entirely annihilated by the New York Revised Statutes. They were also abolished by statute in Connecticut, 1793, and they have never existed, or they have ceased to exist, in all essential respects, in every other state. The only feudal fictions and services to be retained in any part of the United States consist of the feudal principle, that the lands are held of some superior or lord, to whom the obligation of fealty, and to pay a determinate rent, are due. . . . The lord paramount of all socage land was none other than the people of the state, and to them, and them only, the duty of fealty was to be rendered. . . ." 3 James Kent, *Commentaries on American Law* \*509–10 (George Cornstock ed., 11th ed. 1866).

**base tenure.** *Hist.* The holding of property in villeinage rather than by military service or free service. See VILLEINAGE.

**copyhold tenure.** See COPYHOLD.

**lay tenure.** *Hist.* Any tenure not held through religious service, such as a base tenure or a freehold tenure. • The three historical types of lay tenures are *knight-service*, *socage*, and *serjeanty*. See KNIGHT-SERVICE; SOGAGE; SERJEANTY. Cf. *tenure by divine service*.

**military tenure.** A tenure that bears some relation to military service, such as knight-service, grand serjeanty, and cornage. — Also termed *tenure in chivalry*.

**spiritual tenure.** A tenure that bears some relation to religious exercises, such as frankalmoign and tenure by divine service.

**tenure ad furcam et flagellum (ad fər-kəm et flə-jel-əm).** [Latin] *Hist.* Tenure by gallows and whip. • This was the meanest of the servile tenures — the bondman was at the disposal of the lord for life and limb.

**tenure by divine service.** *Hist.* A tenure obligating the tenant to perform an expressly defined divine service, such as singing a certain number of masses or distributing a fixed sum of alms. Cf. *lay tenure*.

**tenure in chivalry.** See *military tenure*.

**villein tenure.** See VILLEINAGE.

3. A status afforded to a teacher or professor as a protection against summary dismissal without sufficient cause. • This status has long been considered a cornerstone of academic freedom. [Cases: Colleges and Universities Ⓒ8.1(2); Schools Ⓒ133.6. C.J.S. *Colleges and Universities* § 24; *Schools and School Districts* §§ 222–223, 226–228, 236–238.] 4. More generally, the legal protection of a long-term relationship, such as employment. [Cases: Officers and Public Employees Ⓒ60. C.J.S. *Officers and Public Employees* §§ 119, 130, 134.] — **tenurial (ten-yūr-ee-əl), adj.**

**tenured faculty.** The members of a school's teaching staff who hold their positions for life or until retirement, and who may not be discharged except for cause. [Cases: Colleges and Universities Ⓒ8.1(2). C.J.S. *Colleges and Universities* § 24.]

**tenure in capite.** See IN CAPITE.

**tenure in chivalry.** See *military tenure* under TENURE.

**teratogen (tə-rat-ə-jən), n.** An agent, usu. a chemical, that causes injury to a fetus or any of various birth defects <alcohol is a teratogen to the developing brain of a fetus>. — **teratogenic (tə-rat-ə-jen-ik), adj.**

**terce.** *Hist. Scots law.* A widow's interest in one-third of her husband's real property, if she has not accepted some other special provision. • The couple must have been married at least a year and a day or else have produced a living child together. See POWER.

**terce land.** *Hist. Scots law.* Income-producing real property in which a widow has a pecuniary interest because it was owned by her husband.

**tercer.** *Hist. Scots law.* A widow who has an interest in one-third of her husband's real property. — Also spelled *tercear*.

**tergiversatio (tər-jiv-ər-say-shee-oh), n.** [Latin "being reluctant, hanging back"] *Roman law.* A delay tactic, esp. an accuser's failure to pursue a criminal charge, perhaps by not appearing at the trial. • To withdraw an accusation, it was necessary to obtain the court's permission for an annulment (*abolitio*). In AD 61, a law was passed by which anyone convicted of *tergiversatio* was subject to a fine. See CALUMNIA. Cf. PRAEVARIATIO. Pl. *tergiversationes* (tər-jiv-ər-say-shee-oh-neez).

**term, n.** 1. A word or phrase; esp., an expression that has a fixed meaning in some field <term of art>. 2. A contractual stipulation <the delivery term provided for shipment within 30 days>. See CONDITION (3).

**essential term.** See *fundamental term*.

**fundamental term.** 1. A contractual provision that must be included for a contract to exist; a contractual provision that specifies an essential purpose of the contract, so that a breach of the provision through inadequate performance makes the performance not only defective but essentially different from what had been promised. [Cases: Contracts Ⓒ9(1), 15. C.J.S. *Contracts* §§ 33, 35–36, 38, 42–43.] 2. A contractual provision that must be included in the contract to satisfy the statute of

frauds. — Also termed *essential term*; *vital term*. [Cases: Frauds, Statute of  $\text{\textcircled{C}}113$ .]

**implied term.** A provision not expressly agreed to by the parties but instead read into the contract by a court as being implicit. • An implied term should not, in theory, contradict the contract's express terms. [Cases: Contracts  $\text{\textcircled{C}}168$ . C.J.S. *Contracts* §§ 346–347.]

**material term.** A contractual provision dealing with a significant issue such as subject matter, price, payment, quantity, quality, duration, or the work to be done. [Cases: Contracts  $\text{\textcircled{C}}9$ . C.J.S. *Contracts* § 42.]

**nonessential term.** See *nonfundamental term*.

**nonfundamental term.** Any contractual provision that is not regarded as a fundamental term. — Also termed *nonessential term*; *nonvital term*. [Cases: Contracts  $\text{\textcircled{C}}9(1)$ , 15. C.J.S. *Contracts* §§ 33, 35–36, 38, 42–43.]

**vital term.** See *fundamental term*.

3. (*pl.*) Provisions that define an agreement's scope, conditions or stipulations <terms of sale>. 4. A fixed period of time; esp., the period for which an estate is granted <term of years>.

**attendant term.** A long period (such as 1,000 years) specified as the duration of a mortgage, created to protect the mortgagor's heirs' interest in the land by not taking back title to the land once it is paid for, but rather by assigning title to a trustee who holds the title in trust for the mortgagor and the mortgagor's heirs. • This arrangement gives the heirs another title to the property in case the interest they inherited proves somehow defective. These types of terms have been largely abolished. See *tenancy attendant on the inheritance* under TENANCY. [Cases: Mortgages  $\text{\textcircled{C}}54$ . C.J.S. *Mortgages* § 102.]

"The advantage derived from attendant terms is the security which they afford to purchasers and mortgagees. If the *bona fide* purchaser or mortgagee should happen to take a defective conveyance or mortgage, by which he acquires a mere equitable title, he may, by taking an assignment of an outstanding term to a trustee for himself, cure the defect, so far as to entitle himself to the legal estate during the term, in preference to any creditor, of whose incumbrance he had not notice, at or before the time of completing his contract for the purchase or mortgage. He may use this term to protect his possessions, or to recover it when lost. This protection extends generally as against all estates and incumbrances created intermediately between the raising of the term and the time of the purchase or mortgage; and the outstanding term, so assigned to a trustee for the purchaser or mortgagee, will prevail over the intermediate legal title to the inheritance." 4 James Kent, *Commentaries on American Law* \*87 (George Comstock ed., 11th ed. 1866).

**satisfied term.** A term of years in land that has satisfied the purpose for which it was created before the term's expiration.

**term for deliberating.** The time given a beneficiary to decide whether to accept or reject an inheritance or other succession.

**term in gross.** A term that is unattached to an estate or inheritance. See *tenancy in gross* under TENANCY.

**term of years.** 1. A fixed period covering a precise number of years. — Also termed *tenancy for a term*.

2. *English law.* A fixed period covering less than a year, or a specified number of years and a fraction of a year. • This sense applies under a seminal English statute — the Law of Property Act of 1925.

"In effect, 'term of years' seems to mean a term for any period having a fixed and certain duration as a minimum. Thus, in addition to a tenancy for a specified number of years (e.g., 'to X for ninety-nine years'), such tenancies as a yearly tenancy or a weekly tenancy are 'terms of years' within the definition, for there is a minimum duration of a year or a week respectively. But a lease 'for the life of X' cannot exist as a legal estate, and the same, perhaps, applies to tenancies at will or at sufferance (if they are estates at all) for their duration is wholly uncertain." Robert E. Megarry & M.P. Thompson, *A Manual of the Law of Real Property* 74 (6th ed. 1993).

5. The period or session during which a court conducts judicial business <the most recent term was busy indeed>. — Also termed (in sense 5) *term of court*. See *SESSION*. [Cases: Courts  $\text{\textcircled{C}}63$ . C.J.S. *Courts* §§ 111–113, 120.]

**additional term.** A distinct, added term to a previous term. [Cases: Courts  $\text{\textcircled{C}}64$ . C.J.S. *Courts* § 119.]

**adjourned term.** A continuance of a previous or regular term but not a separate term; the same term prolonged. [Cases: Courts  $\text{\textcircled{C}}66$ . C.J.S. *Courts* § 115.]

**appearance term.** The regular judicial term in which a party is required to appear, usu. the first one after legal service has been made.

**civil term.** The period during which a civil court hears cases.

**criminal term.** A term of court during which indictments are found and returned, and criminal trials are held.

**equity term.** The period during which a court tries only equity cases.

**general term.** A regular term of court — that is, the period during which a court ordinarily sits. — Also termed *stated term*. [Cases: Courts  $\text{\textcircled{C}}63$ . C.J.S. *Courts* §§ 111–113, 120.]

**regular term.** A term of court begun at the time appointed by law and continued, in the court's discretion, until the court lawfully adjourns. [Cases: Courts  $\text{\textcircled{C}}63$ . C.J.S. *Courts* §§ 111–113, 120.]

**special term.** A term of court scheduled outside the general term, usu. for conducting extraordinary business. [Cases: Courts  $\text{\textcircled{C}}64$ . C.J.S. *Courts* § 119.]

**stated term.** See *general term*.

**term probatory.** *Eccles. law.* 1. The period given to the promoter of an ecclesiastical suit to produce witnesses and prove the case. 2. *Hist.* The time assigned for taking testimony. — Sometimes termed (in sense 2) *probatory term*.

**term to conclude.** *Eccles. law.* A deadline imposed by the judge for all parties to renounce any further exhibits and allegations.

**term to propound all things.** *Eccles. law.* A deadline imposed by the judge for the parties to exhibit all evidence supporting their positions.

6. *Hist. English law.* One of the four periods in a year during which the courts are in session to conduct judicial business. • Terms came into use in the 13th century, and their dates varied. The four terms — Hilary, Easter, Trinity, and Michaelmas — were abolished by the Judicature Acts of 1873–1875, and the legal year was divided into sittings and vacations. Terms are still maintained by the Inns of Court to determine various time periods and dates, such as a call to the bar or observance of a Grand Day.

**term annuity.** See *annuity certain* under ANNUITY.

**term attendant on the inheritance.** See *tenancy attendant on the inheritance* under TENANCY.

**term bond.** See BOND (3).

**term clause.** See HABENDUM CLAUSE (2).

**term day.** See *quarter day* under DAY.

**term fee.** *English law.* A sum that a solicitor may charge a client, and that the client (if successful) may recover from the losing party, payable for each term in which any proceedings following the summons take place.

**term for deliberating.** See TERM (4).

**term for years.** See *tenancy for a term* under TENANCY.

**terminable interest.** See INTEREST (2).

**terminable property.** Property (such as a leasehold) whose duration is not perpetual or indefinite but that is limited in time or liable to terminate on the happening of an event.

**terminal disclaimer.** See DISCLAIMER.

**terminate, vb.** 1. To put an end to; to bring to an end.  
2. To end; to conclude.

**termination, n.** 1. The act of ending something; EXTINGUISHMENT <termination of the partnership by winding up its affairs>.

*termination of conditional contract.* The act of putting an end to all unperformed portions of a conditional contract. [Cases: Contracts ⇨249. C.J.S. *Contracts* §§ 422, 424, 427–428, 456, 465–466, 484.]

*termination of employment.* The complete severance of an employer–employee relationship. [Cases: Master and Servant ⇨21, 22. C.J.S. *Apprentices* § 10; *Employer–Employee Relationship* §§ 41–42, 45, 55.]

2. The end of something in time or existence; conclusion or discontinuance <the insurance policy's termination left the doctor without liability coverage>. — **terminate, vb.** — **terminable, adj.**

**termination clause.** See CANCELLATION CLAUSE.

**termination fee.** A fee paid if a party voluntarily backs out of a deal to sell or purchase a business or a business's assets. • Termination fees are usu. negotiated and agreed on as part of corporate merger or acquisition negotiations. The fee is designed to protect the prospective buyer and to deter the target corporation from entertaining bids from other parties. — Also termed *break-up fee*.

**termination-for-convenience clause.** A contractual provision allowing the government to terminate all or a portion of a contract when it chooses. • Among the governmental contracts that often include a termination-for-convenience clause are service contracts, research-and-development contracts, and fixed-price contracts. See 48 CFR § 52.249-1.

**termination hearing.** See *termination-of-parental-rights hearing* under HEARING.

**termination of parental rights.** *Family law.* The legal severing of a parent's rights, privileges, and responsibilities regarding his or her child. • Termination of a parent's rights frees the child to be adopted by someone else. — Abbr. TPR. See *termination-of-parental-rights hearing* under HEARING; PARENTAL RIGHTS.

**termination proceeding.** An administrative action to end a person's or entity's status or relationship. • For example, the International Banking Act authorizes the International Banking Board to institute a termination proceeding when a foreign bank or its U.S. agency or branch is convicted of money-laundering. 12 USCA § 3105(e).

**terminer.** See OYER AND TERMINER.

**term in gross.** See TERM (4).

**termini habiles** (tər-mi-ni hab-ə-leez), *n.* [Law Latin] *Hist.* Sufficient grounds. • The phrase usu. referred to the facts necessary to establish a prescriptive right.

**termini sanctorum** (tər-mi-ni sangk-tər-əm), *n.* [Law Latin] *Hist.* The limits of a sanctuary. See SANCTUARY (1).

**term interest.** *Oil & gas.* A mineral interest or royalty interest that is not perpetual. • A term interest may be for a fixed term (e.g., for 25 years) or defeasible (e.g., for 25 years and so long thereafter as there is production from the premises).

**terminus ad quem** (tər-mi-nəs ad kwem). [Law Latin] *Hist.* The point to which. • The phrase appeared in reference to the point before which some action must be taken.

**terminus a quo** (tər-mi-nəs ay kwoh). [Law Latin] *Hist.* The point from which. • The phrase appeared in reference to the point from which something is calculated, or the earliest time at which some action is possible.

**term life insurance.** See LIFE INSURANCE.

**term loan.** See LOAN.

**term of art.** 1. A word or phrase having a specific, precise meaning in a given specialty, apart from its general meaning in ordinary contexts. • Examples in law include *and his heirs* and *res ipsa loquitur*. [Cases: Contracts ⇨152; Statutes ⇨192. C.J.S. *Contracts* §§ 307, 318–322, 327, 331; *Statutes* § 322.] 2. Loosely, a jargonistic word or phrase. — Also termed *word of art*.

**term-of-art canon.** In statutory construction, the principle that if a term has acquired a technical or specialized meaning in a particular context, the term should be presumed to have that meaning if used in that context. [Cases: Statutes ⇨192.]

**term of court.** See TERM (5).

**Appendix E:**

Privacy Commissioner of Canada, "Guidance on  
Covert Video Surveillance in the Private Sector"  
(May 2009)



# Office of the Privacy Commissioner of Canada

---

## Reports and Publications

### OPC Guidance Documents

#### Guidance on Covert Video Surveillance in the Private Sector

##### Introduction and scope

The Office of the Privacy Commissioner considers covert video surveillance to be an extremely privacy-invasive form of technology. The very nature of the medium entails the collection of a great deal of personal information that may be extraneous, or may lead to judgments about the subject that have nothing to do with the purpose for collecting the information in the first place. In the Office's view, covert video surveillance must be considered only in the most limited cases.

This guidance is based on the federal private sector privacy law *The Personal Information Protection and Electronic Documents Act* (PIPEDA), and is intended to outline the privacy obligations and responsibilities of private sector organizations contemplating and engaging in covert video surveillance. We consider video surveillance to be covert when the individual is not made aware of being watched.

This document serves as a companion piece to the following guidelines for video surveillance issued by this office: [Guidelines for Overt Video Surveillance in the Private Sector](#) (prepared in collaboration with Alberta and British Columbia) and [Guidelines for surveillance of public places by police and law enforcement authorities](#).

Please note that the following is guidance only. We consider each complaint brought before us on a case-by-case basis.

##### PIPEDA requirements governing covert video surveillance

PIPEDA governs the collection, use and disclosure of personal information in the course of a commercial activity and in the employment context of federally regulated employers<sup>1</sup>. The capturing of images of identifiable individuals through covert video surveillance is considered to be a collection of personal information. Organizations that are contemplating the use of covert video surveillance should be aware of the criteria they must satisfy in order to collect, use and disclose video surveillance images in compliance with PIPEDA. These criteria are outlined below and address the purpose of the covert video surveillance, consent issues, and the limits placed on collecting personal information through covert video surveillance.

A common misconception is that organizations are released from their privacy obligations if covert video surveillance is conducted in a public place. In fact, under PIPEDA, any collection of personal information taking place in the course of a commercial activity or by an employer subject to PIPEDA, regardless of the location, must conform to the requirements described below.

##### A. Purpose

The starting point for an organization that is contemplating putting an individual under surveillance without their knowledge is to establish what purpose it aims to achieve. What is the reason for collecting the individual's personal information through covert video surveillance? Under PIPEDA, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances (subsection 5(3)).

In deciding whether to use covert video surveillance as a means of collecting personal information, an organization should closely examine the particular circumstances of why, when and where it would collect personal information and what personal information would be collected. There are a number of considerations that factor into determining whether an organization is justified in undertaking covert video surveillance. Given the different contexts in which covert video surveillance may be used, the ways in which the factors apply and are analyzed vary depending on the circumstances.

### **Demonstrable, evidentiary need**

In order for the organization's purpose to be considered appropriate under PIPEDA, there must be a demonstrable, evidentiary need for the collection. In other words, it would not be enough for the organization to be acting on a mere suspicion. The organization must have a strong basis to support the use of covert video surveillance as a means of collecting personal information.

### **Information collected by surveillance achieves the purpose**

The personal information being collected by the organization must be clearly related to a legitimate business purpose and objective. There should also be a strong likelihood that collecting the personal information will help the organization achieve its stated objective. The organization should evaluate the degree to which the personal information being collected through covert video surveillance will be effective in achieving the stated purpose.

### **Loss of privacy proportional to benefit gained**

Another factor to be considered is the balance between the individual's right to privacy and the organization's need to collect, use and disclose personal information. An organization should ask itself if the loss of privacy is proportional to the benefit gained. It may decide that covert video surveillance is the most appropriate method of collecting personal information because it offers the most benefits to the organization. However, these advantages must be weighed against any resulting encroachment on an individual's right to privacy in order for a reasonable person to consider the use of covert surveillance to be appropriate in the circumstances.

### **Less privacy-invasive measures taken first**

Finally, any organization contemplating the use of covert video surveillance should consider other means of collecting the personal information given the inherent intrusiveness of covert video surveillance. The organization needs to examine whether a reasonable person would consider covert video surveillance to be the most appropriate method of collecting personal information under the circumstances, when compared to less privacy-invasive methods.

## **B. Consent**

As a general rule, PIPEDA requires the individual's consent to the collection, use and disclosure of personal information (Principle 4.3). It is possible for covert video surveillance to take place with consent. For example, an individual can be considered to have implicitly consented to the collection of their personal information through video surveillance if that individual has initiated formal legal action against the organization and the organization is collecting the information for the purpose of defending itself against the legal action. It is important to note that implied consent does not authorize unlimited collection of an individual's personal information but limits collection to what is relevant to the merits of the case and the conduct of the defence.

In most cases, however, covert video surveillance takes place without consent. PIPEDA recognizes that there are limited and specific situations where consent is not required (paragraph 7(1)(b)). In order to collect information through video surveillance without the consent of the individual, organizations must be reasonably satisfied that:

- collection with the knowledge and consent of the individual would compromise the availability or

accuracy of the information; and

- the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

The exception to the requirement for knowledge and consent could, in certain circumstances, provide for the collection of a third party's personal information.

In the employment context, an organization should have evidence that the relationship of trust has been broken before conducting covert video surveillance. Organizations cannot simply rely on mere suspicion but must in fact have evidentiary justification.

Regardless of whether or not consent is obtained, organizations must have a reasonable purpose for collecting the information.

## C. Limiting collection

When collecting personal information, organizations must take care to limit both the type and amount of information to that which is necessary to fulfill the identified purposes (Principle 4.4). Organizations should be very specific about what kind of personal information they are looking to collect and they should limit the duration and scope of the surveillance to what would be reasonable to meet their purpose. Moreover, the collection must be conducted in a fair and lawful manner.

As well, organizations must limit the collection of images of parties who are not the subject of an investigation. There may be situations in which the collection of personal information of a third party<sup>2</sup> via covert video surveillance could be considered acceptable provided the organization has reason to believe that the collection of information about the third party is relevant to the purpose for the collection of information about the subject. However, in determining what is reasonable, the organization must distinguish between persons who it believes are relevant to the purposes of the surveillance of the subject and persons who are merely found in the company of the subject. In our view, PIPEDA does not allow for the collection of the personal information of the latter group without their knowledge or consent.

Organizations can avoid capturing individuals who are not linked to the purpose of the investigation by being more selective during video surveillance. If such personal information is captured, it should be deleted or depersonalized as soon as is practicable. This refers not only to images of the individuals themselves, but also to any information that could serve to identify them, such as street numbers and licence plates. We advocate the use of blurring technology when required. Though we acknowledge its cost to organizations, we view the expenditure as necessary given that, pursuant to PIPEDA, the personal information of any individual can only be collected, used and disclosed without consent in very limited and specific situations.

## The need to document

Proper documentation by organizations is essential to ensuring that privacy obligations are respected and to protect the organization in the event of a privacy complaint. Organizations should have in place a general policy that guides them in the decision-making process and in carrying out covert video surveillance in the most privacy-sensitive way possible. There should also be a documented record of every decision to undertake video surveillance as well as a record of its progress and outcome.

### 1. Policy on covert video surveillance

Organizations using covert video surveillance should implement a policy that:

- sets out privacy-specific criteria that must be met before covert video surveillance is undertaken;
- requires that the decision be documented, including rationale and purpose;
- requires that authorization for undertaking video surveillance be given at an appropriate level of the organization;

- limits the collection of personal information to that which is necessary to achieve the stated purpose;
- limits the use of the surveillance to its stated purpose;
- requires that the surveillance be stored in a secure manner;
- designates the persons in the organization authorized to view the surveillance;
- sets out procedures for dealing with third party information;
- sets out a retention period for the surveillance; and
- sets out procedures for the secure disposal of images.

## 2. Documenting specific instances of video surveillance

There should be a detailed account of how the requirements of the organization's policy on video surveillance have been satisfied, including:

- a description of alternative measures undertaken and their result;
- a description of the kind of information collected through the surveillance;
- the duration of surveillance;
- names of individuals who viewed the surveillance;
- what the surveillance was used for;
- when and how images were disposed of; and
- a service agreement with any third party hired to conduct the surveillance, if applicable.

## Best practices for using private investigation firms

Many organizations hire private investigation firms to conduct covert video surveillance on their behalf. It is the responsibility of both the hiring organization and the private investigation firm to ensure that all collection, use and disclosure of personal information is done in accordance with privacy legislation. We strongly encourage the parties to enter into a service agreement that incorporates the following:

- confirmation that the private investigation firm constitutes an "investigative body" as described in PIPEDA "Regulations Specifying Investigative Bodies";
- an acknowledgement by the hiring organization that it has authority under PIPEDA to collect from and disclose to the private investigation firm the personal information of the individual under investigation;
- a clear description of the purpose of the surveillance and the type of personal information the hiring organization is requesting;
- the requirement that the collection of personal information be limited to the purpose of the surveillance;
- the requirement that the collection of third party information be avoided unless the collection of information about the third party is relevant to the purpose for collecting information about the subject;
- a statement that any unnecessary personal information of third parties collected during the surveillance should not be used or disclosed and that it should be deleted or depersonalized as soon as is practicable;
- confirmation by the private investigation firm that it will collect personal information in a manner

consistent with all applicable legislation, including PIPEDA;

- confirmation that the private investigation firm provides adequate training to its investigators on the obligation to protect individuals' privacy rights and the appropriate use of the technical equipment used in surveillance;
- the requirement that the personal information collected through surveillance is appropriately safeguarded by both the hiring organization and the private investigation firm;
- the requirement that all instructions from the hiring company be documented;
- a provision prohibiting the use of a subcontractor unless previously agreed to in writing, and unless the subcontractor agrees to all service agreement requirements;
- a designated retention period and secure destruction instructions for the personal information;
- a provision allowing the hiring company to conduct an audit.

<sup>1</sup> For information on whether your organization is subject to PIPEDA, please see "A Guide for Business and Organizations" online at [http://www.priv.gc.ca/information/guide\\_e.cfm](http://www.priv.gc.ca/information/guide_e.cfm)

<sup>2</sup> By "third party", we mean the person who is not the subject of surveillance.

*May 2009*

---

Date Modified: 2009-05-27

**Appendix F:**

Information and Privacy Commissioner of Alberta,  
Privacy Commissioner of Canada, and Information  
and Privacy Commissioner for British Columbia,  
“Guidelines for Overt Video Surveillance in the  
Private Sector (March 2008)”



## Guidelines for Overt Video Surveillance in the Private Sector March 2008

### FEDERAL

Privacy Commissioner  
of Canada

### PROVINCIAL

Information and  
Privacy Commissioner  
of Alberta

Information and  
Privacy Commissioner  
for British Columbia

### Introduction

The use of video surveillance by private sector organizations has exploded in recent years. As technology has evolved and costs have fallen dramatically, video surveillance is increasingly accessible to a large range of organizations. Security and crime control concerns are the most common motivating factors for the deployment of video surveillance cameras. Retailers use cameras in hopes of deterring thefts and identifying suspects. Cameras are installed in apartment buildings to detect vandalism and increase the security of tenants. But there are other less obvious uses as well. Some retailers conduct video surveillance to analyze consumer behaviour – which store aisles they frequent, where they stop, what products they examine.

Private sector privacy laws require that organizations' need to conduct video surveillance must be balanced with the individuals' right to privacy, which includes the right lead their lives free from scrutiny. Given its inherent intrusiveness, organizations should consider all less privacy-invasive means of achieving the same end before resorting to video surveillance.

To help organizations achieve compliance with private sector privacy legislation, we have developed these Guidelines, which set out the principles for evaluating the use of video surveillance and for ensuring that its impact on privacy is minimized. These Guidelines apply to overt video surveillance of the public by private sector organizations in publicly accessible areas. These Guidelines *do not* apply to covert video surveillance, such as that conducted by private investigators on behalf of insurance companies, nor do they apply to the surveillance of employees.

An important note – private sector privacy laws<sup>1</sup> govern the collection, use and disclosure of information about an identifiable individual. In the private sector, surveillance through a video camera is subject to privacy laws. Under PIPEDA and the Alberta and British Columbia *PIPA*s, the information does not need to be recorded.

---

<sup>1</sup> *Personal Information Protection and Electronic Documents Act (PIPEDA)*  
*Alberta's Personal Information Protection Act (PIPA)*  
*British Columbia's Personal Information Protection Act (PIPA)*  
*Quebec's An Act Respecting the Protection of Personal Information in the Private Sector*

## **10 things to do when considering, planning and using video surveillance**

1. Determine whether a less privacy-invasive alternative to video surveillance would meet your needs.
2. Establish the business reason for conducting video surveillance and use video surveillance only for that reason.
3. Develop a policy on the use of video surveillance.
4. Limit the use and viewing range of cameras as much as possible.
5. Inform the public that video surveillance is taking place.
6. Store any recorded images in a secure location, with limited access, and destroy them when they are no longer required for business purposes.
7. Be ready to answer questions from the public. Individuals have the right to know who is watching them and why, what information is being captured, and what is being done with recorded images.
8. Give individuals access to information about themselves. This includes video images.
9. Educate camera operators on the obligation to protect the privacy of individuals.
10. Periodically evaluate the need for video surveillance.

### **Qs and As**

**Q.** What can we use video surveillance for?

**A.** There are a number of situations where it may be reasonable to expect video surveillance to take place, for example, for security purposes around banking machines or inside convenience stores in high-crime areas. In areas where people have a much higher expectation of privacy, such as a public washroom or a spa treatment room, video surveillance is inappropriate.

When considering the use of video surveillance, make sure that all less privacy invasive alternatives have been looked at. It is preferable to first put the appropriate security measures in place, such as placing inventory under lock and key.

**Q.** What are we allowed to do with the information we obtain through video surveillance?

**A.** Information collected through video surveillance should only be used for the purpose that surveillance is being undertaken, or for purposes that are permitted by law. For example, if cameras are installed in an apartment building parking garage for safety purposes, the information cannot be used to track the movements of tenants. However, if a car is broken into, the information can be disclosed to law enforcement.



**Q.** What should we keep in mind when installing and operating the cameras?

**A.** The video surveillance system should be set up and operated to collect the minimum amount of information to be effective. This helps reduce the intrusion on individuals' privacy. Specifically:

- Cameras that are turned on for limited periods in the day are preferable to "always on" surveillance.
- Cameras should be positioned to reduce capturing images of individuals who are not being targeted. For example, a store security camera should not be recording passersby outside the store.
- Cameras should not be aimed at areas where people have a heightened expectation of privacy, for example, showers or into windows. Steps should be taken to ensure that cameras cannot be adjusted or manipulated by the operator to capture images in such areas.
- Sound should not be recorded unless there is a specific need to do so.
- If a camera is monitored, the recording function should be turned on only when unlawful activity is suspected or observed.

Organizations should also ensure that the video surveillance complies with all applicable laws, in addition to privacy legislation. For example, an organization using a video camera that captures sound needs to consider the *Criminal Code* provisions dealing with the collection of private communications.

**Q.** Should we post signs that there are cameras in operation?

**A.** Yes. Most privacy laws require the organization conducting video surveillance to post a clear and understandable notice about the use of cameras on its premises to individuals whose images might be captured by them, *before* these individuals enter the premises. This gives people the option of not entering the premises if they object to the surveillance. Signs should include a contact in case individuals have questions or if they want access to images related to them.

**Q.** What are our responsibilities with regard to recorded images?

**A.**

- The recorded images must be stored in a secure location, and access should be granted only to a limited number of authorized individuals.
- Individuals have the right to access images relating to them. When disclosing recordings to individuals who appear in them, the organization must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity.
- Any disclosure of video surveillance recordings outside the organization should be justified and documented.
- Recordings should only be kept as long as necessary to fulfill the purpose of the video surveillance. Recordings no longer required should be destroyed. Organizations must ensure that the destruction is secure.

**Q.** What are our obligations to the people who operate our video surveillance system?

**A.** Organizations should ensure that appropriate and ongoing training is provided to operators to make certain that they:

- understand their obligations under all relevant legislation, these Guidelines, and the organization's video surveillance policy; and
- conduct surveillance only for the purposes identified by the organization.

**Q.** Once the video surveillance system is up and running, what do we need to do to ensure continued compliance with privacy laws?

**A.** Organizations should evaluate all aspects of the operation of their video surveillance system regularly. In particular, organizations should examine whether video surveillance continues to be required and should consider:

- Was video surveillance effective in addressing the problem for which it was introduced?
- Does the problem still exist?
- Would a less intrusive way of addressing the problem now be effective?

**Q.** How should my organization document the use of video surveillance?

**A.** Organizations should develop a policy on video surveillance that sets out:

- the rationale and purpose of the surveillance system;
- the location and field of vision of the equipment;
- any special capabilities of the system, for example, sound, zoom, facial recognition or night-vision features;
- the rationale and purpose of the specific locations of equipment and fields of vision selected;
- the personnel authorized to operate the system and access the information it contains;
- the times when surveillance will be in effect;
- whether and when recording will occur;
- the place where signals from the equipment will be received and monitored;
- guidelines for managing video surveillance recordings, including security, use, disclosure, and retention;
- procedures for the secure disposal of video surveillance recordings;
- a process to follow if there is unauthorized disclosure of images;
- procedures for individuals to access personal information captured and challenge any suspected failure to comply with the policy;
- sanctions for the organization's employees and contractors for failing to adhere to the policy; and
- the individual accountable for privacy compliance and who can answer any questions about the surveillance.

**Appendix G:**

Dr. Ann Cavoukian, "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report", Privacy Investigation Report MC07-68 (March 30, 2007)

# **Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report**

**Privacy Investigation Report  
MC07-68**

**March 3, 2008**





## Table of Contents

<b>Introduction .....</b>	<b>1</b>
<b>Background.....</b>	<b>1</b>
<b>Privacy and Video Surveillance.....</b>	<b>2</b>
<b>Evidence of the Effectiveness of Video Surveillance .....</b>	<b>3</b>
Discussion of the Empirical Research on Video Surveillance .....	7
Conclusions from the Empirical Research on Video Surveillance.....	10
<b>Why Video Surveillance is Believed to Enhance Public Safety .....</b>	<b>10</b>
<b>Emerging Privacy-Enhancing Video Surveillance Technology.....</b>	<b>12</b>
<b>Innovative Privacy-Enhancing Approach .....</b>	<b>13</b>
<b>Conduct of the Investigation .....</b>	<b>15</b>
Extent of Surveillance .....	15
Operation of the System .....	16
Public Consultation.....	17
<b>Issues Arising in the Investigation .....</b>	<b>18</b>
<b>Summary of Conclusions.....</b>	<b>43</b>
<b>Recommendations .....</b>	<b>44</b>
<b>Commissioner’s Message.....</b>	<b>45</b>

---

## Introduction

The significant growth of video surveillance cameras throughout the world, especially as witnessed in the United Kingdom, has created considerable concerns with respect to privacy. This Report was prompted by a complaint received from Privacy International regarding the Canadian expansion of the use of video surveillance cameras in the City of Toronto's mass transit system. In light of the divergent points of view on video surveillance, in addition to investigating this complaint, my office decided to expand our Report to include a review of the literature, as well as an examination of the role that privacy-enhancing technologies can play in mitigating the privacy-invasive nature of video surveillance cameras. As such, this Report is longer than most, attempting to provide a comprehensive analysis examining the broader context of video surveillance. Given the enormous public support for the use of video surveillance cameras in mass transit systems and by the law enforcement community, addressing this issue broadly, with a view to seeking a positive-sum paradigm through the use of privacy-enhancing technologies, is our ultimate goal.

## Background

On October 24, 2007, the Office of the Information and Privacy Commissioner of Ontario (IPC) received a letter of complaint from an organization relating to the deployment of video surveillance cameras throughout the Toronto Transit Commission's (TTC) mass transit system in Toronto, Ontario. The organization subsequently publicly identified itself as Privacy International, which is based in the United Kingdom.<sup>1</sup>

The letter of complaint expressed the view that the TTC's use of video surveillance cameras contravened the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). In their letter, Privacy International argued that the collection principles of the *Act* "are not being sufficiently attended to in that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers." It argued that the program has been undertaken on the basis of crime prevention and crime detection despite the fact that there is no evidence that video surveillance on public transit systems significantly reduces the level of crime or the threat of terrorist attacks. It also argued that studies indicate that video surveillance has a marginal impact on investigations and that video surveillance cameras are plagued with technological and management issues. Finally, Privacy International stated that the TTC had failed to respect legal requirements for public consultation, disclosure and establishment of a public interest case for its video surveillance system. In order to address these issues, this privacy complaint file was opened (MC07-68), and an investigation commenced.

Before outlining the investigation of this complaint, I will first provide background information on the privacy implications of video surveillance cameras and the manner in which these issues have been addressed by my office, over the years. I will also include a discussion of the research

---

<sup>1</sup> The letter of complaint has been posted to Privacy International's website: [http://www.privacyinternational.org/issues/compliance/complaint\\_ttc\\_privacy.pdf](http://www.privacyinternational.org/issues/compliance/complaint_ttc_privacy.pdf).

on the effectiveness of video surveillance, since this is a pivotal issue in this investigation. For those who may only be interested in the investigation itself, please proceed directly to that part of the report dealing with the specifics of the investigation, beginning on page 15.

## Privacy and Video Surveillance

Historically, pervasive video surveillance has posed a threat to privacy and constitutional rights. When controlled by government departments, video surveillance can provide the government with massive amounts of personal information about the activities of law-abiding citizens, going about their daily lives. When individuals know they are being watched, this may have a chilling effect on their freedom to speak, act and associate with others. Since individuals may censor their own activities when they are aware of being watched, video surveillance may also be perceived as a means of enforcing social conformity.

Privacy and the right of individuals to go about their daily activities in an anonymous fashion not only protects freedom of expression and association, but also protects individuals from intrusions into their daily lives by the government. Accordingly, when government organizations wish to use surveillance technology in a manner that will impact the privacy of all citizens, there must be clear justification for doing so. Specifically, the benefits of the technology should justify any invasion of privacy.

It has been argued that individuals cannot have a reasonable expectation of privacy in public places, especially in the case of urban mass transit systems where large volumes of people may be concentrated in relatively restricted spaces. In addition, it has been argued that video surveillance in such places is an enhancement of a person's natural ability to observe what is happening in public. While the expectation of privacy in public spaces may be lower than in private spaces, it is not entirely eliminated. People *do* have a right to expect the following: that their personal information will only be collected for legitimate, limited and specific purposes; that the collection of their personal information will be limited to the minimum necessary for the specified purposes; and that their personal information will only be used and disclosed for the specified purposes. These general principles should apply to all video surveillance systems.

In order to address situations where government organizations elect to deploy video surveillance systems, my office issued *Guidelines for the Use of Video Surveillance Cameras in Public Places* (the *Guidelines*), in 2001. These *Guidelines* were later updated in 2007,<sup>2</sup> and are based on the provisions of Ontario's *Freedom of Information and Protection of Privacy Act* and its municipal counterpart, the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*). Since they were issued, the *Guidelines* have been used by many government organizations to develop and implement video surveillance programs in a privacy-protective manner, in compliance with the *Acts*.

The *Guidelines* are intended to assist organizations in determining whether the collection of personal information by means of video surveillance is lawful and justifiable as a policy choice,

---

<sup>2</sup> These *Guidelines* are available online: [http://www.ipc.on.ca/images/Resources/up-3video\\_e\\_sep07.pdf](http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf).

and if so, how privacy-protective measures may be built into the system. The *Guidelines* do not apply to covert surveillance, or surveillance when used as a case-specific investigation tool for law enforcement purposes, where there is statutory authority and/or the authority of a search warrant to conduct the surveillance.

Before deciding whether to use video surveillance, the *Guidelines* recommend that organizations consider the following:

- A video surveillance system should only be adopted after other measures to protect public safety or to deter, detect, or assist in the investigation of criminal activity have been considered and rejected as unworkable. Video surveillance should only be used where conventional means (e.g., foot patrols) for achieving the same law enforcement or public safety objectives are substantially less effective than surveillance or are not feasible, and the benefits of surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.
- The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- An assessment should be made of the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects may be mitigated.
- Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public.
- Organizations should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

Once a decision has been made to deploy video surveillance, the *Guidelines* set out the manner in which video surveillance cameras should be implemented in order to minimize their impact on privacy.

I have taken these *Guidelines* into consideration in investigating the TTC's video surveillance program.

## Evidence of the Effectiveness of Video Surveillance

In its letter of complaint, Privacy International made reference to empirical studies addressing the efficacy of video surveillance. Since there is considerable disparity in the views relating to its efficacy, my office decided to conduct a selective review of the literature on the effectiveness of video surveillance on potential offenders and on criminal justice processes and outcomes. The focus of the review was on research conducted over the past 10 years.



The literature review found numerous studies on the effectiveness of video surveillance on crime, in a broad range of settings. These studies varied substantially, however, in terms of their methodological rigor. Since an in-depth review of each of these studies was not feasible within the course of our investigation, we decided to rely on the work of credible experts who evaluated a broad range of studies on the topic and drew their conclusions on the basis of the quality of the empirical evidence before them.

There are significant challenges to conducting high quality research on video surveillance in natural settings because of the difficulty of controlling the multitude of extraneous factors that may influence the research outcomes. In order to demonstrate the effectiveness of video surveillance on crime prevention, a study would have to show either a decrease in the rate of crime, or a slowing in an increasing crime rate in locations where video surveillance cameras had been implemented. To confirm that any such change was attributable to video surveillance, a study would have to show that a similar decrease in crime or a slowing in the increasing crime rate did not occur in comparable locations where video surveillance cameras had not been implemented (control areas). In addition, in order to confirm that such changes in crime rates were long-term as opposed to transient, the evaluation period would have to extend for a substantial period of time. Unfortunately, research with this level of methodological rigor is extremely rare.

In 1997, California-based Marcus Nieto examined whether the use of video surveillance in public and private places was effective in preventing crime and concluded that the data suggested that the technology was successful in both reducing and preventing crimes, and was helpful in prosecuting individuals caught in the act of committing a crime.<sup>3</sup> Nieto looked at evaluations of the technology from around the world.

In 2001, in its *Final Report: Evaluation of the NSW Government Policy Statement and Guidelines for Closed Circuit Television (CCTV) in Public Places*, the Inter-departmental Committee on video surveillance reported on an evaluation of video surveillance technology throughout New South Wales, Australia.<sup>4</sup> The committee concluded that the anecdotal reports and statistics provided an indication that video surveillance may be effective in certain contexts and had received a high level of support. However, the committee noted that none of the assessments could be viewed as systematic evaluations of the technology.

In 2003, the Royal Canadian Mounted Police commissioned an evaluation of the effects of video surveillance systems on crime.<sup>5</sup> Wade Deisman, Professor of Criminology and Director of the multidisciplinary National Security Working Group at the University of Ottawa, conducted the evaluation. The review showed that “the effects of video surveillance on crime are quite

---

3 See Marcus Nieto, “Public video surveillance: is it an effective crime prevention tool?” Sacramento: California Research Bureau, California State Library, June 1997.

4 See “Final report: evaluation of the NSW government policy statement & guidelines for closed circuit television (CCTV) in public places”, prepared for the Inter-Departmental Committee on CCTV c/o Crime Prevention Division, Attorney General’s Department, July 2001 online: <http://www.dlg.nsw.gov.au/Files/Information/CCTV%20final%20report.PDF>

5 See Wade Deisman, “CCTV: literature review and bibliography”, Research and Evaluation Branch, Community, Contract and Aboriginal Policing Services Directorate, Royal Canadian Mounted Police, 2003, available online by request: [http://www.rcmp-grc.gc.ca/ccaps/cctv\\_e.htm](http://www.rcmp-grc.gc.ca/ccaps/cctv_e.htm)

variable and fairly unpredictable”<sup>6</sup> and that the deterrent value of video surveillance varies over time and across crime categories. Video surveillance systems were found to have the least effect on public disorder offences.<sup>7</sup> The magnitude of the deterring effects of video surveillance on crime was found to depend on the location, with the greatest benefit being in parking lots. The evaluation also found that video surveillance cameras did not need to be operational in order to deter crime. The deterring effects were highest when video surveillance was used in conjunction with other crime reduction measures and when tailored to the local setting. Continuing publicity was also required to maintain the positive effects of video surveillance systems on crime, over time. No evidence was found of increased conviction rates with the implementation of video surveillance.

In 2002, the Home Office in the United Kingdom issued a report entitled, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*.<sup>8</sup> The report was written by Brandon Welsh, Professor in the Department of Criminal Justice at the University of Massachusetts Lowell, and David Farrington, Professor of Psychological Criminology in the Institute of Criminology at the University of Cambridge. The authors assessed 46 relevant studies from both the United States and Britain according to strict methodological criteria and found that only 22 studies were rigorous enough to include in their analysis. On the basis of these 22 studies, they concluded that video surveillance reduced crime to a small degree and was most effective at reducing vehicle crime in parking lots. Video surveillance was found to have little or no effect on crime in public transport and city centre settings.

In 2005, the Home Office in the United Kingdom issued another report on a study of the effectiveness of video surveillance systems.<sup>9</sup> Martin Gill, Professor of Criminology at the University of Leicester, directed the evaluation. The report provides a systematic evaluation of 13 video surveillance projects implemented in a range of contexts, including town centres, city centres, parking lots, hospitals and residential areas. The results were contradictory – crime went down in some target areas while it went up in others. Video surveillance systems installed in mixed category areas (e.g., parking lots, a hospital, etc.) showed the greatest reduction in crime, particularly in parking lots. Impulsive crimes, such as alcohol-related ones were found to be less likely to be reduced than premeditated crimes, such as auto theft. Violence tended to increase while auto theft tended to decrease, in accordance with trends in national crime statistics.

It is important to note that regardless of the inconclusiveness of the empirical research on the effectiveness of video surveillance, the Home Office in the United Kingdom has not been deterred from supporting the use of this technology. A report issued in October 2007 entitled *National CCTV Strategy* stated that video surveillance plays a significant role in protecting the public and assisting the police in the investigation of crime.<sup>10</sup> It went on to state that the technology

---

6 *Ibid*, page 2.

7 Public disorder offences may include acts of violence and/or intimidation by individuals or groups of individuals, such as rioting and drunkenness.

8 See Brandon C. Welsh and David P. Farrington, “*Crime prevention effects of closed circuit television: a systematic review*”, Home Office Research Study 252 online: <http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>

9 See Martin Gill and Angela Spriggs, “*Assessing the Impact of CCTV*”, Home Office Research Study 292, February 2005 online: <http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>

10 See Graeme Gerrard, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill and Sarah Douglas, “*National CCTV Strategy*”, Home Office, October 2007 online: <http://www.crimereduction.homeoffice.gov.uk/cctv/cctv048.pdf>

has been instrumental in helping the police to identify and bring to justice those involved in all aspects of criminality, including serious crimes and terrorist incidents. The report noted that the contribution that video surveillance has made to the protection of the public and assisting the police in investigating crime has been realized despite the fact that the technology has been “developed in a piecemeal fashion with little strategic direction, control or regulation.”<sup>11</sup> The report recommended the development of a strategy to maximize the potential of the video surveillance infrastructure.

In 2006, the United States’ Department of Justice, Office of Community Oriented Policing Services issued a report entitled *Video Surveillance of Public Places*.<sup>12</sup> The report was written by Jerry Ratcliffe, Professor in the Department of Criminal Justice at Temple University. The report provides an overview of video surveillance systems, explores the benefits and problems associated with the technology, and summarizes the findings of numerous evaluations.

The report notes that while there is a general perception among system managers and the public that video surveillance cameras are effective in preventing crime, actual evidence of crime reduction is more difficult to find. Nevertheless, based on the evidence provided by several evaluation reviews, the general findings were as follows:

- Video surveillance is more effective at reducing property crime than violent or public order crime (although there have been some successes in this area);
- Video surveillance appears to work best in small, well-defined areas (such as public parking lots);
- The individual context and the way the system is used appear to be important;
- Achieving statistically significant reductions in crime is difficult due to normal fluctuations in crime rates;
- The involvement of the police is an important determinant of the success of a system; and
- There is an investigative benefit to video surveillance once an offense has been committed.

In summary, the author concluded that, “it is possible to say there was some evidence of crime reduction in most of the systems . . . there is a growing list of evaluations that suggest CCTV has had some qualified successes in reducing crime.”<sup>13</sup>

---

11 *Ibid*, page 5.

12 See Jerry Ratcliffe, “*Video Surveillance of Public Places*”, Problem-Oriented Guides for Police, Response Guides Series No. 4, U.S. Department of Justice, Office of Community Oriented Policing Services, 2006 online: <http://www.cops.usdoj.gov/mime/open.pdf?Item=1693>

13 *Ibid*, page 20.

## Discussion of the Empirical Research on Video Surveillance

It should be noted that applications of video surveillance vary widely in many aspects. This makes it difficult to make comparisons across studies and to draw general conclusions from the evaluations. For example, applications vary in terms of the following:

- the goals of the applications;
- types of video surveillance technology used;
- passive versus active monitoring of videos;
- types of target areas (e.g., closed versus open);
- size of the target areas;
- density of cameras;
- fixed versus redeployable cameras; and
- involvement of law enforcement.

In addition, while the empirical evidence in support of the effectiveness of video surveillance in combating crime is weaker than might be expected, it is important to note that most of the research has been carried out in the United Kingdom, where video surveillance technology has proliferated, in part, due to substantial amounts of federal government funding. In contrast, the introduction of video surveillance cameras in Ontario has been more selective as it has not yet received large scale funding from either the federal or provincial governments. Since research shows that situational factors influence the effectiveness of video surveillance cameras, the research findings from other jurisdictions, such as the United Kingdom, may not be directly applicable in the Ontario context.

For example, while video surveillance systems have shown little effect on crime in town centres and city centres in the United Kingdom, a study of the effectiveness of video surveillance cameras on crime in Sudbury, Ontario showed very positive results.<sup>14</sup> Specifically, the study found that after the first camera was installed, crime rates in the downtown area dropped dramatically. It was estimated that between 300 and 500 robberies, assaults, thefts and other criminal offenses have been deterred by the video surveillance project, saving as much as \$800,000 in direct monetary losses. In addition, arrests relating to prostitution and drug offenses increased by an average of 18 percent per year, as a direct result of enhanced capacity to detect these crimes. The authors concluded that the video surveillance system had been effective in both deterring and detecting crime.

The discrepancy between the findings in the United Kingdom and those in Ontario could be due to situational variations in the application of the technology. For example, one could speculate that video surveillance systems may be deployed in a more strategic manner in locations where

---

14 See “*Evaluation of Lion’s Eye in the Sky Video Monitoring Project*”, KPMG, 2000.

funding for such initiatives is scarce. This may result in greater reductions in local crime rates in such locations when compared to locations where funding is more abundant.

It is also important to note that the research on the effectiveness of video surveillance has been plagued by methodological flaws, most notably the following:

- Lack of suitable control areas (i.e., areas where crime rates have not been influenced by the implementation of other crime prevention measures during the study period);
- Lack of adequate crime statistics (e.g., statistics may not be isolated to the targeted area);
- Crime rates may not be reliable indicators due to changes in the definitions of crimes and changes in the way crimes are reported over time (i.e., individuals may be less inclined to report crimes if they believe there are video surveillance cameras in the area or individuals may be more inclined to report crimes if they believe the police will be able to apprehend criminals due to the availability of video surveillance images that may be used as evidence);
- No assessment of displacement or diffusion of benefits into surrounding areas;
- Inadequate pre- and post-video surveillance time periods in which data are collected;
- The fact that video surveillance may actually increase the detection of certain types of crimes thereby driving reported crime rates up;
- Many evaluations involved dated video surveillance technology that may be less useful for identifying offenders in comparison to the newer video surveillance technology;
- Video surveillance is seldom implemented in isolation – it is usually implemented as one component of a package of crime prevention measures and therefore its effects are difficult to isolate;
- Cameras are sometimes located in target areas with crime rates that are too low to notice a difference following the implementation of video surveillance cameras;
- Video surveillance cameras are often implemented in a piecemeal manner, making it difficult to compare crime statistics before and after implementation;
- Crime rates vary naturally over time and show evidence of seasonality and long and short-term trends, making it difficult to isolate the effects of video surveillance cameras and making it difficult to obtain statistically significant results;
- Lack of clear objectives for implementing video surveillance cameras, making it difficult to find suitable effectiveness measures;

- Offenders may not be aware of the presence of cameras, making it virtually impossible to deter crime; and
- Very little of the research has been conducted by independent third parties.

Unfortunately, there are no clear conclusions to be drawn. There are substantial challenges in finding statistically significant evidence that video surveillance reduces crime and aids in criminal justice processes. However, it is equally difficult to conclude from the ambiguous findings reported in the literature that video surveillance is not, in fact, effective in deterring criminal activity. This conclusion is supported by other evidence on the effectiveness of video surveillance, particularly in the detection and investigation of crime, which is clearly much less equivocal than the research on the effects of video surveillance in deterring crime.

For example, in 1993, video surveillance images of toddler Jamie Bulger being led away from a Merseyside shopping mall by his two 10-year-old abductors assisted the police in identifying and apprehending his murderers.<sup>15</sup> Video surveillance footage released to the public led to early identification of suspects and played an important role in their subsequent prosecution in the case of the Brixton nail bomber in 1999 and in the failed bombing of London's subway system on July 21, 2005. In the later case, four men were found guilty of conspiracy for murder for their involvement.<sup>16</sup> More recently, images collected from video surveillance cameras located in a hospital in Sudbury, Ontario were highly instrumental in identifying and locating a woman who pleaded guilty to having kidnapped a newborn infant from the hospital.<sup>17</sup> Images collected from the camera were very helpful in the return of the infant to his family.

The efficiency with which video surveillance footage has been used in the investigation of terrorism in London dramatically altered perceptions about video surveillance. For example, Nigel Brew, in a research note entitled *An Overview of the Effectiveness of Close Circuit Television (CCTV) Surveillance*, prepared for the government of Australia in 2005, concluded that "video surveillance may be of more value as a source of evidence than as a deterrent."<sup>18</sup> However, as argued by Michael Greenberger, Director of the University of Maryland Centre for Health and Homeland Security, following the terrorist attacks in 2005, the "effective investigatory use of CCTV is very likely to be a significant deterrence to future terrorist activities on London mass transit."<sup>19</sup>

---

15 See the article by Shirley Lynn Scott, "The Video Tape" at the Crime Library website online: [http://www.crimelibrary.com/notorious\\_murders/young/bulger/4.html](http://www.crimelibrary.com/notorious_murders/young/bulger/4.html)

16 See "4 Guilty in Failed 2005 London Bombing" New York Times, July 9, 2007, online: <http://www.nytimes.com/2007/07/09/world/europe/09cnd-london.html?hp>

17 See "Woman pleads guilty to Sudbury baby abduction" CanWest News Service, November 24, 2007, online: <http://www.nationalpost.com/news/story.html?id=121816>

18 See Nigel Brew, "An overview of the effectiveness of closed circuit television (CCTV) surveillance", Research Note no. 14 2005-06, Parliament of Australia, Foreign Affairs, Defense and Trade Section. October 28, 2005, page 6 online: <http://www.aph.gov.au/Library/pubs/rn/2005-06/06rn14.htm>

19 See the Abstract for Michael Greenberger, "The need for closed circuit television in mass transit systems", Law Enforcement Executive Forum. 6(1), 2006 online: <http://www.umaryland.edu/healthsecurity/docs/CCTV%20in%20Mass%20Transit%20Systems.pdf>

## Conclusions from the Empirical Research on Video Surveillance

Since the bulk of the empirical research is deficient in a number of respects, it is difficult to draw any definitive conclusions about the effectiveness of video surveillance cameras. Without an ability to control the many factors that influence outcomes and the context and mechanisms that produce these outcomes, it is not surprising that the results of earlier evaluations have been mixed, conflicting and, at times, contradictory. Video surveillance systems do not appear to have uniform effects across a wide range of crime categories. At present, it is difficult to find unequivocal evidence that video surveillance deters or prevents crime. However, it is equally difficult to conclude the opposite. A more valuable role for video surveillance may be as a source of evidence in the detection and investigation of crime. A much larger body of research, with a consistent degree of methodological rigor, is needed before definitive statements may be made.

## Why Video Surveillance is Believed to Enhance Public Safety

Historically, video surveillance was most often implemented in public spaces because of an expectation of crime deterrence.<sup>20</sup> In general, the goal of deterrence and crime prevention strategies is to put in place practices or conditions that will lead potential offenders to refrain from engaging in criminal activities, delay criminal actions, or avoid a particular target. As is the case with many crime prevention strategies, video surveillance aims to make the potential offender believe that there is an increased risk of apprehension. To increase the perception of risk, the potential offender must be aware of the presence of the cameras and believe that the cameras present sufficient risk of capture to outweigh the rewards of the intended crime. Awareness of the cameras may be enhanced through public education, clear signage, and media coverage of incidents caught on camera. In addition to awareness, however, understanding the consequences of being caught by the cameras requires rational thought. It is unlikely that potential offenders under the influence of drugs or alcohol would be deterred from acts of violence or public disorder by the presence of cameras.

Video surveillance is also believed to reduce crime by helping in the detection, arrest and prosecution of offenders. When an incident occurs in the presence of video surveillance cameras, the police can respond quickly and in a manner that is more appropriate to the situation. To the extent that offenders are captured and convicted using video surveillance evidence, this may prevent them from committing further crimes.

While video surveillance has contributed to the apprehension of criminals in a number of high profile cases, historically its value has stemmed from its potential to deter rather than detect criminal activity. This view is now changing. The value in detecting crimes is now being considered as a primary goal of video surveillance.

---

<sup>20</sup> See Jerry Ratcliffe, “*Video Surveillance of Public Places*”, Problem-Oriented Guides for Police, Response Guides Series No. 4, U.S. Department of Justice, Office of Community Oriented Policing Services, 2006 online: <http://www.cops.usdoj.gov/mime/open.pdf?Item=1693>

Video surveillance images may also assist the police in investigating crimes. It is important to note that video surveillance footage may not only help the police identify offenders, but may also help in the identification of potential witnesses who may otherwise be reluctant to come forward.

In addition, video surveillance is believed to make people feel more safe and secure. This is an important goal of security programs for all mass transit systems. If members of the public do not feel secure, they may avoid using public transit, thereby decreasing ridership.

In short, there are reasons other than deterrence, as to why video surveillance may help to prevent crime and aid the police in criminal investigations. This may help to explain why video surveillance systems are strongly supported and continue to proliferate.



## Emerging Privacy-Enhancing Video Surveillance Technology

While technology is essentially privacy neutral, if deployed without careful consideration to its impact on privacy, it may be extremely invasive. I have been a strong advocate for harnessing the strengths of technology and putting them in the service of privacy – enlisting the support of technology to enhance, instead of erode, privacy. Privacy enhancing technologies (PETs) are those information and communication technologies that incorporate measures to protect privacy by eliminating or reducing the collection, retention, use and disclosure of personal information. This is often referred to as “data minimization” and increasingly represents a vital component of privacy protection.

To avoid the costly and ineffective retrofitting of technology to address privacy issues after they have been implemented, it is essential that privacy protections be built directly into their design and implementation, right from the outset. This view is captured in my mantra of “privacy by design.” It is incumbent upon those who wish to deploy surveillance systems to be aware of and adopt PETs whenever possible, especially as they become commercially available.

Recent research has shown that it is possible to design surveillance systems in a manner that may successfully address issues of public safety, while at the same time, protecting the privacy of law-abiding citizens.

There are a variety of technologies based on digital image processing that are currently being researched and developed for protecting the privacy of individuals appearing in video surveillance footage. As described in the research literature, these approaches are operating as follows:

Step 1: object detection and segmentation methods for locating objects of interest, such as human faces, within images and video frames; and

Step 2: object obscuration or securing methods, which after the completion of step 1, manipulate the pixel data so that some or all viewers of the surveillance footage are unable to discern the private object content (which one is seeking to protect from viewing).

For the first step, object detection and segmentation, there are many well established approaches using pattern recognition algorithms, some of which are currently used in surveillance and recognition systems. For the second step, object obscuration or securing, there are various approaches, the choice of which is dependent upon the application requirements. The simplest approach is to blur or discard (i.e., obscure with a black box) the private object content. The significant limitation of this approach is that the content is irretrievable for future investigative purposes if it is applied immediately during acquisition of the surveillance footage. What is needed is a novel privacy-enhancing approach that allows the personally identifiable information or objects of interest in the original video stream to be securely protected from viewing, while at the same time, preserving the original content stream and enabling this information to be retrieved at a later date, if required.

## Innovative Privacy-Enhancing Approach

I am delighted to report that at the University of Toronto, Karl Martin and Kostas Plataniotis, have developed such a privacy-enhancing approach to video surveillance. Their work, as described in *Privacy Protected Surveillance Using Secure Visual Object Coding*,<sup>21</sup> uses cryptographic techniques to secure a private object (personally identifiable information), so that it may only be viewed by designated persons of authority, by unlocking the encrypted object with a secret key. In other words, objects of interest (e.g. a face or body) are stored as completely separate entities from the background surveillance frame, and efficiently encrypted. This approach represents a significant technological breakthrough because by using a secure object-based coding approach, both the texture (i.e. content) and the shape of the object (see Figure (b) below), or just the texture (see Figure (c) below) may be encrypted.<sup>22</sup> Not only is this approach more flexible, but the encryption used is also more efficient than existing approaches that encrypt the entire content stream. This allows designated persons to monitor the footage for unauthorized activity while strongly protecting the privacy of any individuals caught on tape. Upon capture of an incident that requires further investigation (i.e., a crime scene), the proper authorities can then decrypt the object content in order to identify the subjects in question. The decryption may be performed either in real-time or on archived footage. Since the encryption is performed in conjunction with the initial coding of the objects, it may be performed during acquisition of the surveillance footage, thus reducing the risk of any circumvention.

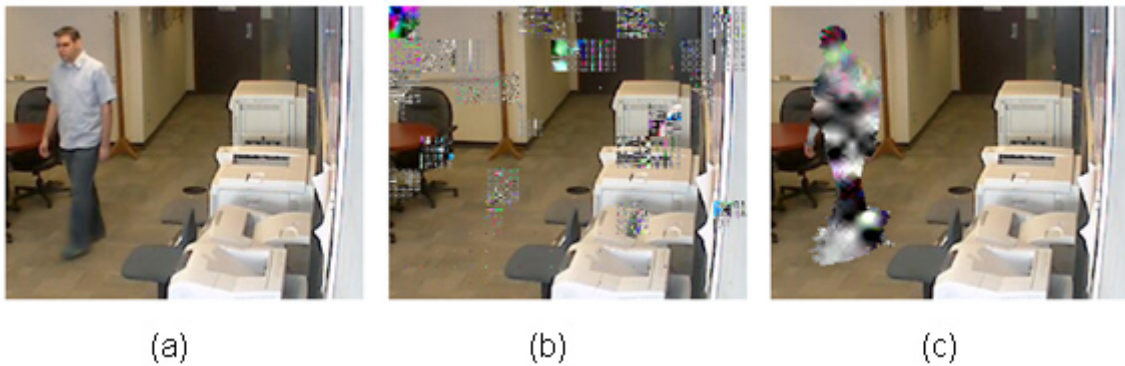


Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.

<sup>21</sup> See Karl Martin and Konstantinos N. Plataniotis, “*Privacy protected surveillance using secure visual object coding*”, the Edward S. Rogers Sr. Dept. of Electrical and Computer Engineering, University of Toronto, Multimedia Lab Technical Report 2008.01 online: [http://www.dsp.utoronto.ca/~kmartin/papers/tech\\_report\\_2008.01-surveillance](http://www.dsp.utoronto.ca/~kmartin/papers/tech_report_2008.01-surveillance)

<sup>22</sup> The figure contains a photograph of one of the researchers. The researcher in the photograph consented to its publication in this Report.

## The Pitfalls of a Zero-Sum Approach

Over the years, I have argued that adopting a zero-sum paradigm, where one party wins and one party loses, is ultimately shortsighted and least effective. As a result, my office has developed “positive-sum” models for consideration in the use of emerging technologies where both parties may “win” and neither party must, by necessity, lose. In the scenario involving video surveillance cameras, the police may have a legitimate goal in using video surveillance cameras as a tool in the detection of criminal activity, while, at the same time, individuals have a legitimate expectation that their daily activities will not be monitored and preserved on tape. The innovative work of Martin and Plataniotis provides an ideal example of a positive-sum technology, where both interests can prevail: Video surveillance cameras may be deployed for reasons consistent with public safety and law enforcement, however, no personal information from camera footage is accessible to unauthorized parties, not in possession of the decryption key. Strong policies would need to be implemented in conjunction with this technology to restrict access to the decryption key to a limited number of authorized individuals. Protocols should also be developed governing the conditions under which video surveillance footage could be decrypted, for example, only after a crime had been committed or a safety mishap had occurred.

The use of this type of privacy-enhancing technology would thus allow for video surveillance to be conducted without the usual concerns associated with this type of surveillance. For the great majority of the surveillance footage, there would be absolutely no access or viewing of any personally identifiable information and, no unauthorized activities, such as viewing out of curiosity or “leering,” would be possible.<sup>23</sup> Therefore, this privacy-enhancing technology would enable both the use of video surveillance cameras *and* privacy to co-exist, side by side – without forfeiting one for the other: positive-sum, not zero-sum.

---

23 See Jeffrey Rosen’s seminal book “*The Naked Crowd*”, 2004 for examples of video surveillance voyeurism where unsupervised video surveillance camera operators in the United Kingdom entertained themselves by zooming in on attractive young women or couples engaged in sexual activities.

In this book, he argues that it is possible to strike an effective balance between liberty and security by adopting well-designed laws and technologies.

## Conduct of the Investigation

As discussed above, in its letter of complaint to the IPC, Privacy International raised concerns regarding the TTC's deployment of video surveillance cameras and asserted that the TTC's use of video surveillance was not in accordance with the privacy provisions of the *Act*. Privacy International's letter made reference to past studies on the efficacy of video surveillance, technological concerns regarding the use of video surveillance, as well as legal considerations.

In order to provide the TTC with the opportunity to respond to the issues raised in the complaint, my office met with their staff. I also wrote to the TTC to confirm my understanding of the background facts pertaining to this complaint and to obtain the TTC's written representations on whether the operation of the video surveillance system was in accordance with the provisions of the *Act*. The TTC provided a thorough and detailed response. Privacy International was also provided with an opportunity to submit additional information, but declined to do so.

Staff from my office also conducted a site visit to examine the video surveillance system in place at a representative TTC subway station.

## Extent of Surveillance

The TTC indicated that there are currently cameras in both the TTC's subway system and on its surface vehicles (which are comprised of buses and streetcars). With respect to the TTC's fleet of 1,750 surface vehicles, 286 buses are fully equipped with four cameras on each bus, for a total of 1,144 cameras. (To date, no cameras have been installed on streetcars). With respect to the TTC's subway system, there are currently 1,200 cameras located throughout the 69 stations. These cameras are generally located at choke points (major access points), Designated Waiting Areas, automatic entrances, elevators, collector booths, and other site-specific areas of concern.

The TTC expressed its plans to expand its surveillance program on both surface vehicles and within the subway system. Specifically, the TTC plans to equip its remaining 1,464 surface vehicles with cameras so that all surface vehicles will have cameras by the end of 2008. With four cameras planned for each vehicle, this would amount to a total of 5,856 cameras on the TTC's entire fleet of surface vehicles. In addition, there are plans to install five cameras per vehicle on all 144 Wheel Trans vehicles (a total of 720 cameras) by the end of 2008. With respect to the subway system, the TTC plans to increase the number of cameras on the subway system by 1,100, from the current number of 1,200, to a total of 2,300 by the end of 2011. In addition, the TTC plans to introduce cameras inside subway cars. Currently, there are plans to install a total of 1,014 cameras on 39 new subway train sets that will begin to be introduced into the TTC system in late 2009.

It is our understanding that all of the existing and proposed cameras are or will be located in places where they have the potential to capture images of individuals.

## Operation of the System

The TTC has also provided background information on the operation of the cameras. Specifically, the TTC has provided information about the retention of video surveillance images; the type of technology used; the monitoring of live video surveillance images; and access to recorded video surveillance images on both surface vehicles and within the subway system.

With respect to retention schedules, the TTC explained that recorded video surveillance images from surface vehicles are retained for a period of 15 hours, at which time they are automatically overwritten. For the cameras operating in subway stations, the recorded video surveillance images are retained for a maximum period of up to seven days, at which time they are automatically overwritten.

With respect to the type of video surveillance technology used, the TTC indicated that the cameras located on surface vehicles all utilize digital technology. The cameras currently located within the subway system utilize both analog and digital technology.

With respect to the active monitoring of the video surveillance images, the TTC stated that the cameras located on surface vehicles are not monitored nor are the images accessible by the vehicle drivers. The only way that video surveillance images from surface vehicles could be actively monitored from a remote location would be through a wireless video surveillance network. Such a network has not been installed by the TTC. With respect to the subway system, the TTC noted that, while these cameras are not generally monitored, cameras from 16 subway stations are currently linked through a fibre-optic cable that permits live remote access to video surveillance images by four departments of the TTC: Transit Control, Signals/ Electrical/Communications Maintenance Department, Signals/Electrical/Communications Engineering Department, and Special Constable Services. The purposes for which each of these departments may access the live video surveillance images is described below.

With respect to Transit Control, although the live feed and monitors are “on” 24 hours a day in case a problem arises within the subway system, the video surveillance images are not actively monitored. Transit Control determines which subway platforms are monitored through the live feed. Approximately eight cameras can be displayed at one time. With respect to both Signals/Electrical/Communications Engineering and Maintenance Departments, the cameras are not actively monitored. Remote access to the video surveillance signals is used strictly for maintenance-related issues, such as system failure, camera failure, network failure or preventative maintenance. Special Constable Services also do not actively monitor the live video surveillance feed. All access is strictly logged and incident-driven.

In addition to the live video surveillance feed from cameras linked to the fibre-optic cable, there is a live feed to monitors that are viewable by a TTC Superintendent on weekdays during the morning and evening rush hours. The live feed monitors the subway platforms at crossover stations, where the north-south subway line meets the east-west subway line. The live video surveillance images are used strictly for the purpose of monitoring overcrowding on the platforms to ensure passenger safety. If necessary, public announcements are made by the Superintendent to provide updates or directions to passengers.

Currently, with respect to access to recorded video surveillance images, from both surface vehicles and the subway system, when an incident has taken place, an investigator must isolate and copy the images prior to the expiration of the retention period in order to use them during the course of an investigation. The ability to access and download recorded video surveillance images is therefore strictly controlled. Investigations may be conducted internally by the TTC, or by an external law enforcement agency, such as the Toronto Police Services.

In addition, once a Memorandum of Understanding (MOU) is signed between the Toronto Police Services Board and the TTC, the Police will have direct remote access to the recorded video surveillance images collected in the subway system. All access to the video surveillance images will be incident driven and require a case file number. Access will be limited to eight individuals within the Video Services Unit. All access will be fully logged.

The TTC's operation of the video cameras is governed by their "Video Recording Policy," (the Policy) which has been provided to my office in draft form. The Policy is not yet complete and has not been officially adopted by the TTC. Once in force, the Policy will address all major aspects of the TTC's usage of their cameras, including:

- a statement of the program's rationale and objectives;
- the responsibilities of various job designations within the TTC regarding the surveillance system;
- the requirement that Notice of Collection be provided to all TTC passengers whose images are collected through the surveillance cameras;
- procedures for responding to a potential privacy breach; and
- acceptable retention periods for recorded images.

## **Public Consultation**

The TTC stated that it has engaged in various forms of public consultation on video surveillance at different points in time. For instance, with respect to cameras within the subway system, during the design of the Sheppard Subway Extension, a Personal Security Design Review Group (PSDRG) was created in order to provide input into security features of the new subway line, including the installation of cameras. The TTC stated that the PSDRG was comprised of various public interest groups including the Toronto Safe City Committee and the Metro Action Committee on Public Violence against Women.

With respect to the use of video surveillance cameras in new subway cars, the TTC stated that it had conducted a public viewing of a mock-up of the new subway cars from June 6 to July 21, 2006 and had invited the public to comment on its features, including the use of video surveillance cameras.

For the cameras planned on streetcars, the TTC also noted that it has been involved in a public consultation with respect to the purchase of new streetcars. Among other things, this public consultation dealt with the potential installation of video surveillance cameras. In addition, the TTC stated that recommendations relating to the purchase of additional cameras for surface vehicles have been the subject of public reports,<sup>24</sup> and that any group wishing to provide feedback on such reports would have the option of doing so at a TTC Commission meeting.

## Issues Arising in the Investigation

I have identified the following issues arising from this investigation, each of which will be discussed in turn.

- (A) Is the information collected by the TTC’s video surveillance cameras “personal information” as defined under section 2(1) of the *Act*?
- (B) Is the collection of personal information by the TTC’s video surveillance cameras in compliance with section 28(2) of the *Act*?
- (C) Is the Notice of Collection provided to passengers in compliance with section 29(2) of the *Act*?
- (D) Is the disclosure of personal information to the Toronto Police Services in compliance with section 32 of the *Act*?
- (E) Does the TTC have adequate security measures in place to safeguard the personal information collected?
- (F) Does the TTC have proper destruction processes in place for recorded information that is no longer in use?
- (G) Does the TTC have proper retention periods in place for personal information that is collected?
- (H) Has the TTC undertaken all appropriate steps prior to implementing video surveillance?
- (I) Is the TTC’s video surveillance system subject to regular audits?

---

24 See the TTC website: <http://www.ttc.ca/postings/gso-comrpt/>

## **Issue A: Is the information collected by the TTC’s video surveillance cameras “personal information” as defined under section 2(1) of the Act?**

In order for a given record of personal information to be subject to the privacy provisions of the *Act*, it must qualify as “personal information” under the definition set out in section 2(1). Section 2(1) of the *Act* states, in part:

“personal information” means recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, telephone number, fingerprints or blood type of the individual,
- (e) the personal opinions or views of the individual except if they relate to another individual,
- (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- (g) the views or opinions of another individual about the individual, and
- (h) the individual’s name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual; ... .

[emphasis added]

The *Guidelines* state:

Personal information is defined in section 2 of the *Acts* as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual’s race, colour, national or ethnic origin, sex and age. If a video surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered “personal information” under the *Acts*.<sup>25</sup>

---

25 See *Guidelines*, page 2.



In this case, the records at issue are the images of individuals that are captured by cameras situated within the TTC system. Clearly, such images are capable of identifying particular individuals and therefore, constitute “recorded information about an identifiable individual.”

I am satisfied that the records in question qualify as “personal information” under section 2(1) of the *Act*. I note that the TTC concurs with this position.

**Conclusion:** The information collected by the TTC’s video surveillance cameras qualifies as “personal information” as defined under section 2(1) of the *Act*.

**Issue B: Is the collection of personal information by the TTC’s video surveillance cameras in compliance with section 28(2) of the *Act*?**

In its letter of complaint to the IPC, Privacy International focused on the issue of whether the TTC’s collection of personal information through the video surveillance cameras was permissible under the *Act*, and stated:

In this complaint we argue that the collection principles are not being sufficiently attended to in that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers.

The section of the *Act* that addresses the collection of personal information is section 28(2), which establishes a basic prohibition on the collection of personal information, but states that there are three circumstances under which the collection of personal information may take place. Section 28(2) states:

No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

In order for a particular collection practice to be in accordance with the *Act*, it must be shown to satisfy at least one of the three conditions set out in section 28(2). In other words, the institution must show that the collection of personal information is either, (1) expressly authorized by statute, (2) used for the purposes of law enforcement, or (3) necessary to the proper administration of a lawfully authorized activity.

The first step in the section 28(2) analysis is to address whether any of the above conditions apply to a given collection of personal information. In this case, the TTC has not provided reference to a statute that provides the express authorization for the collection of personal information through video surveillance. Accordingly, the first condition does not apply.

With respect to the remaining two conditions, in its letter of complaint to the IPC, Privacy International stated that the primary area of focus should be the third condition, which can also be referred to as the “necessity condition.” In its letter, Privacy International made reference

to the Ontario Court of Appeal's decision in *Cash Converters Canada Inc. v. Oshawa (City)*<sup>26</sup> (*Cash Converters*) in stating:

We understand that this is arguably a law enforcement activity and therefore legal exemptions exist for some data privacy principles, as under s.28(2) of MFIPPA. Recently the Ontario Court of Appeal ruled, in *Cash Converters Canada Inc. v. Oshawa (City)*, that where identifiable information is made available to the police it must first meet the necessity condition “where the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity”. When it is possible to find other ways of achieving the stated lawful goals then the institution must choose another route. We do not believe that the TTC has adequately addressed the necessity of this information collection and has not considered access policies.

While the necessity condition is certainly applicable to this investigation, an additional condition that should be considered is the second condition of 28(2), which permits the collection of personal information that is used for the purposes of law enforcement (the law enforcement condition). In the *Cash Converters* decision, the law enforcement condition was not applicable because the collection of personal information at issue was a collection pursuant to a municipal by-law of the City of Oshawa. Under Ontario's *Municipal Act*, a municipality is not permitted to enact a by-law for the purpose of law enforcement. Therefore, consideration of the second condition was not an option. That is not the case in the present investigation.

I will now proceed to consider the application of both the necessity condition and the law enforcement condition in section 28(2) of the *Act*.

#### *Necessary to the Proper Administration of a Lawfully Authorized Activity (The Necessity Condition)*

In *Cash Converters*, the Ontario Court of Appeal adopted the approach my office has taken in the past with respect to the application of the necessity condition and stated:

In cases decided by the Commissioner's office, it has required that in order to meet the necessity condition, the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not “necessary” within the meaning of the *Act*. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route.<sup>27</sup>

Based on the test established by my office, and adopted by the Court of Appeal, in order to satisfy the necessity condition, the institution must first identify the “lawfully authorized activity” in question, and second, it must demonstrate how the collection of personal information is “necessary,” not merely helpful, to the achievement of this objective. In addition, this justification must be provided for all classes of personal information that are collected.

---

26 2007 ONCA 502.

27 *Ibid*, at para. 40.

In this case, the “activity” in question is the operation of a public transit system by the TTC. The TTC is lawfully authorized to operate under Part XVII of the *City of Toronto Act, 2006* which provides that the TTC has the exclusive authority to establish, operate or maintain “a local passenger transportation system within the City.” Therefore, in order to satisfy the necessity condition under section 28(2), the TTC must demonstrate that its collection of personal information through use of video surveillance cameras is necessary to the proper operation of a public transportation system within the City of Toronto.

In considering whether the necessity condition has been satisfied, I have reviewed the documentation provided by the TTC, the information contained in the letter of complaint provided by Privacy International and the research on the topic discussed earlier in this Report. In addition, during the course of the investigation, my office found additional information pertaining to video surveillance in mass transit systems which I have also taken into consideration in determining the necessity of the collection. All of this documentation is discussed below.

Video surveillance is not a new phenomenon in mass transit systems. For years, public transit systems in North America have relied on video surveillance cameras to improve their operations and to enhance public safety and security.

It has been widely recognized that safety and security are essential to the proper functioning of mass transportation systems.<sup>28</sup> Six relevant goals have been proposed for any mass transit security system:

- Awareness of the risks to employees and users of the system, including the nature, level and impact of each risk;
- Mitigation of each risk to the greatest extent possible and an understanding of the nature of any unmitigated risks;
- Awareness of all threats to the proper functioning of the system and mitigating those risks to the greatest extent possible;
- Development of appropriate responses to risk events, both during and after such events;
- Understanding the perceptions and concerns of employees, users, and potential users of the system; and
- Responding to concerns about safety and security through actions and communications.<sup>29</sup>

Typically, mass transit systems have multiple locations, are distributed over large areas, are complex, and have a high volume of passengers. These features of transit systems conspire to make it extremely difficult to achieve the necessary safety and security goals. Video surveillance

---

<sup>28</sup> See, for example, B.M. Finn, “*Keeping an Eye on Transit*”, The Institute of Electrical Engineers, 2004 and Michael Greenberg, “*The need for closed circuit television in mass transit systems*”, Law Enforcement Executive Forum. 6(1), 2006 online: <http://www.umaryland.edu/healthsecurity/docs/CCTV%20in%20Mass%20Transit%20Systems.pdf>

<sup>29</sup> See B.M. Finn, “*Keeping an Eye on Transit*”, The Institute of Electrical Engineers, 2004, page 12.

is viewed as an essential tool for helping to fulfill some of these security goals. Video surveillance is said to serve a number of key functions within mass transit systems, namely:

- Prevention of accidents by monitoring overcrowding, monitoring of individuals in dangerous situations, and monitoring of individuals who may be a danger to themselves;
- Organization of the movement of individuals to avoid bottlenecks and to ensure smooth passenger flows;
- Prevention of crime, public disorder and terrorist acts by monitoring crowd and individual behaviour, and directing security personnel; and
- Assisting in the investigation of incidents by determining how they occurred, identifying potential offenders and witnesses; and providing evidence of criminal or possible terrorist activities.<sup>30</sup>

With respect to the TTC in particular, the Operator Assault Task Force, consisting of representatives of the TTC and the Amalgamated Transit Union Local 113, was created in 2002 in response to statistics indicating an increase in the number of operator assaults in the Toronto transit system. In 2005, the Task Force issued a report that recommended the implementation of video surveillance cameras on all buses and streetcars to assist in preventing operator assaults.<sup>31</sup>

On January 28, 2008, a major newspaper, the Toronto Star, reported on an investigation into the impact of work-related stress on TTC bus, streetcar and subway operators.<sup>32</sup> During the Toronto Star investigation, the reporters obtained information about occupational injury and disease reports filed with the Workplace Safety and Insurance Board, over a five-year period ending in 2005. The investigation, which included interviews with TTC drivers, revealed that at least 181 drivers had filed claims for post-traumatic stress disorder, missing an average of 49 days of work. Post-traumatic stress disorder, associated with the witnessing or experiencing of a traumatic event involving the threat of injury or death, was found to be the second leading cause of lost workdays at the TTC. Drivers were found to have suffered a wide range of abuse on the job – being shot at, spat on, punched, head-butted, slashed with broken bottles, swarmed, kicked and beaten, to name a few examples. The rate of post-traumatic stress disorders among drivers was found to be four times higher than that of Toronto police officers. An additional 102 TTC operators reported missing weeks or months of work due to anxiety, neurotic disorders and depression. TTC operators were found to report these disorders more often than any other workers in Ontario. The Toronto Star investigation also revealed that the number of reported crimes on TTC property had increased dramatically from 2,744 in 2005 to 3,415 in 2006 – an increase of 24 per cent.

As part of the critical infrastructure of modern societies, it is generally accepted that mass transit systems are viewed as highly desirable targets for terrorists. Consequently, in addition to dealing with operator assaults and crime at the local level, mass transit systems have found themselves more recently in a position of having to address issues of national security. Accordingly, video

---

30 *Ibid*, page 13.

31 See the TTC's "Operator Assault Task Force Report of Findings", 2005.

32 See the Toronto Star, "TTC drivers in crisis: Star investigation finds frequent abuse at work puts them at high risk of stress disorder", January 21, 2008.

surveillance cameras within mass transit systems are being upgraded and expanded to deal with the increased potential of a terrorist threat.

On March 20, 1995, subways in Tokyo, Japan were the target of a poison gas attack, an act of domestic terrorism perpetrated by members of Aum Shinrikyo.<sup>33</sup> In five coordinated attacks, the perpetrators released sarin gas on several lines of the Tokyo Metro, killing 12 people, severely injuring 50 and causing vision problems for nearly 1,000 others. The attack was directed against trains passing through Kasumigaseki and Nagatachō, home to the Japanese government.

More recent high profile attacks on public transit systems in Europe underscore this potential terrorist threat. In March 2004, there was a series of coordinated bombings against the commuter train system of Madrid, Spain, killing 191 people and wounding 1,755. On July 7, 2005, there was a series of coordinated terrorist bomb blasts that hit London's public transport system during the morning rush hour. At 8:50 a.m., three bombs exploded within 50 seconds of each other on three London subway trains. A fourth bomb exploded on a bus nearly an hour later at 9:47 a.m. in Tavistock Square. The bombings killed 52 commuters and four suicide bombers, injured 700, and caused disruption of the city's transport system (severely for the first day), as well as immobilizing the country's mobile telecommunications infrastructure.

With respect to the TTC, in 2004 there were two national security investigations involving activities within the Toronto subway system. At that time, upgrades to the TTC security system were recommended by the Chief of the Toronto Polices Services. This recommendation was supported by the Royal Canadian Mounted Police (RCMP) Integrated Security Enforcement Team. In addition, an independent security consultant had recommended the implementation of a system-wide surveillance system for each station and all subway cars following a terrorism-specific risk and vulnerability assessment of the TTC.

The reports, studies and investigations discussed above provide compelling evidence that public safety and security needs on mass transit systems in general, and operator assaults and crime within Toronto's public transit system in particular, represent a pressing and substantial societal concern. I will now proceed to assess whether video surveillance would, in fact, address this pressing and substantial societal concern.

In May of 2001, prior to the terrorist events on September 11<sup>th</sup>, the National Center for Transit Research issued a report outlining the results of a survey of transit agencies throughout the United States with respect to the issue of operator assaults and public safety.<sup>34</sup> Of the 32 agencies that responded to the survey, the majority (26) reported having some type of surveillance system in place. Surveillance cameras in public transit systems were found to be implemented for one or more of the following reasons:

- Crime prevention and response
- Risk management

---

33 Aum Shinrikyo was a religious organization that turned to terrorist tactics, apparently to hasten the apocalypse.

34 See Patricia Maier and Jud Malone, "*Electronic surveillance technology on transit vehicles: a synthesis of transit practice*", Transit Cooperative Research Program, TCRP Synthesis 38, 2001 online: <http://onlinepubs.trb.org/onlinepubs/tcrp/tsyn38.pdf>

- Response to events in progress
- Customer service
- Employee security and other employee-related issues
- Legal evidence

By far, the great majority of transit agencies that used video surveillance (all but one surveyed), indicated that they would recommend the technology to other agencies. Agencies that responded to questions about the effectiveness of surveillance in reducing incidents of crime, rated their systems as being above average. Many reported measurable reductions in the number of assaults and incidents of vandalism. In response to the question relating to the effectiveness of surveillance in achieving criminal convictions, agencies rated their systems as being somewhat better than average. The majority of agencies also reported increases in both riders' and operators' perceptions of security linked to the use of video surveillance.

The TTC conducted a survey of 26 transit agencies in North America regarding the use of video surveillance cameras on transit vehicles.<sup>35</sup> The vast majority of the transit agencies that participated in the survey reported very positive outcomes with video surveillance, including the following: dramatic decreases in crime, reductions in operator and customer assaults, reductions in fraudulent insurance claims, reductions in complaints, improved perceptions of security, the identification, apprehension, and prosecution of suspects in criminal investigations, and the control of student behaviour problems.

In order to determine the use and effectiveness of the existing video surveillance cameras in the Toronto subway system for investigating crimes, the TTC examined requests from law enforcement investigators for information, during the period from January 2007 through July 2007.<sup>36</sup> The study found that 86 per cent of the law enforcement investigators who responded reported that the video images provided positive investigative value. Further, 38 per cent of the respondents indicated that the suspect or suspects caught on camera were successfully apprehended as a result of the images that had been retrieved through the video surveillance cameras.

In the United States, the Department of Homeland Security (DHS) has taken several steps to manage risk and strengthen their nation's rail and transit systems, including offering grants to state and local governments for programs and equipment to help manage this risk. Training and deploying manpower and assets for high risk areas, developing and testing new technologies, and performing security assessments of systems across the country are other measures being taken by the department. Similarly, the Canadian government has also allocated funding for transit security that will "improve security for all who use urban transit in Canada."<sup>37</sup> Video surveillance is viewed as one of the mechanisms of a broader program to address these security issues on mass transit systems.

---

35 A copy of the report on this evaluation was provided to the IPC in the TTC's representations.

36 A summary of this research was provided to the IPC in the TTC's representations.

37 See Transport Canada's new release, "*Canada's new government invests \$37 million to improve transit security in six urban areas*," November 14, 2006 available online: <http://www.tc.gc.ca/mediaroom/releases/nat/2006/06-h138e.htm>

The United States government's funding for security programs and state and local government use of these funds for video surveillance programs was the subject of a DHS workshop held on December 17-18, 2007. The department was seeking input into best practices for states that receive funding for video surveillance installations that would assist the government in ensuring the protection of privacy and civil liberties. A broad range of perspectives were represented at the conference, held in Washington, D.C. On one side of the spectrum, civil liberties groups argued that public video surveillance systems threatened privacy, especially when used in combination with other technologies (e.g., data mining, GPS tracking, RFID, internet, heat sensing video), and have a real potential to change the relationship between the public and the government.<sup>38</sup> On the other side of the debate, law enforcement and emergency management groups noted the need for video surveillance as a key tool to deter criminals; support apprehension and investigation; increase perceptions of safety; promote commerce; and aid in prosecutions.

Interestingly, however, one of the areas in which there was general agreement and acceptance of video surveillance was in the area of mass public transit. The view was that in light of the extensive areas involved (tunnels, platforms, stairways), the high numbers of passengers (especially during rush hours) and the around the clock operating hours of the system, the ability to deal with security issues could not feasibly be limited to increasing the number of security personnel. It was widely acknowledged that one or more cameras could easily cover far more territory than one human being. Similarly, there was general agreement that it would be extremely cumbersome (and impractical) to install a screening mechanism like those existing in airports. Consequently, the views of both privacy advocates and those in emergency management and law enforcement converged on the need for video surveillance in urban mass transit systems – all agreed that the use of video surveillance cameras in this context was justifiable.<sup>39</sup>

There was also another use of video surveillance that did not appear to be particularly objectionable to civil libertarians and privacy advocates, namely the use of such surveillance for the purpose of workplace safety. As noted above, workplace safety, particularly with respect to operator assaults, has been a key issue for the TTC.

Consistent with the views expressed above, there is also evidence to suggest that the general public recognizes that video surveillance may be justifiable in certain high risk locations and that there is a difference between real-time versus archived video surveillance. For example, in one study conducted by Christopher Slobogin, 190 people who had been called for jury duty in Gainesville, Florida were presented with 20 scenarios of video surveillance by the police.<sup>40</sup> The subjects were asked to assume that the target of the surveillance was innocent of any criminal activity. They were then asked to rate the “intrusiveness” of the surveillance on a scale of 1 to 100, with 1 being “not intrusive” and 100 being “very intrusive.” Subjects rated the video surveillance of national monuments and transportation centers, such as airports and train stations, as being minimally invasive (M=20). On average, video surveillance of streets with the tapes destroyed after 96 hours was rated slightly above the middle on the intrusiveness scale (M=53), while

---

38 See Mark Scholosber and Nicole A. Ozer, “*Under the watchful eye: the proliferation of video surveillance systems in California*,” The California American Civil Liberties Union Affiliates, August 2007, online: [http://www.aclunc.org/docs/criminal\\_justice/police\\_practices/Under\\_the\\_Watchful\\_Eye\\_The\\_Proliferation\\_of\\_Video\\_Surveillance\\_Systems\\_in\\_California.pdf](http://www.aclunc.org/docs/criminal_justice/police_practices/Under_the_Watchful_Eye_The_Proliferation_of_Video_Surveillance_Systems_in_California.pdf)

39 Conclusions based on extensive discussions with Washington conference panelists.

40 Slobogin, Christopher, “*Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*” Mississippi Law Journal, Vol. 72, 2002, online: <http://ssrn.com/abstract=364600>

street surveillance without the destruction of tapes was rated as being significantly more intrusive (M=73). This supports the position that the public may not view video surveillance in mass transit systems as being unreasonable, especially if the tapes are destroyed within a reasonable time frame. This study is relevant in the context of the present investigation since the TTC does not actively monitor live video surveillance images and recorded video surveillance images are destroyed after a short retention period, unless they are used for an investigation. Thus, the type of video surveillance being undertaken in the Toronto transit system seeks to minimally impact privacy rights, and may not be perceived as being highly invasive by the general public.

The TTC also noted that the use of video surveillance cameras by transit authorities is quite common, not only in Canada, but around the world. With respect to Canada, the TTC provided information demonstrating that the transit authorities in both Montreal and Vancouver are deploying rail-based video surveillance systems that are far broader in scope than what is being planned for the TTC's subway system.<sup>41</sup>

In its letter of complaint to the IPC, Privacy International stated, with respect to the TTC's video surveillance system, "that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers." I have considered these claims in light of the materials provided by the TTC in response to this complaint and the other documentation cited in this Report. I will address the issues of privacy protocols and access powers in the latter sections of this Report.

To support its position that the collection of information through video surveillance in the Toronto public transit system is unnecessary and disproportionate, Privacy International has disputed the TTC's claim that the expanded video surveillance system would reduce the incidence of crime, while also improving counter-terrorism measures. Specifically, Privacy International referred to a report on a pilot project launched in the Berlin underground.<sup>42</sup> An interim report on the effectiveness of the scheme found that video surveillance did not reduce the incidence of criminality, but rather led to a small increase.

After reviewing an English translation of this study, I noted a number of shortcomings: the time frame for the evaluation of the pilot project was extremely short (i.e., five months); while video surveillance may not have reduced the rate of crime, it was successful in achieving other safety and security objectives, such as documenting attacks on employees. Recall that the objectives of video surveillance in mass transit systems are multifaceted, going beyond finding reductions in crime. Further, the challenges in finding statistically significant reductions in crime rates, in any particular evaluation study, have already been discussed at length earlier in this Report.

Privacy International also pointed to research conducted in the United Kingdom to demonstrate the lack of effectiveness of video surveillance in preventing crime and providing investigatory evidence. While I agree that video surveillance may not be a "silver bullet" in this regard, I again note that there are broader goals for its use in mass transit systems and that, given the massive scope of such systems, there are few viable alternatives. A combination of measures, each with their own recognized limitations, is, in my view (and that of many security experts), the best

---

41 The research was summarized in the TTC's representations to the IPC.

42 See the article "*Study shows video surveillance on the Berlin underground has not improved safety*", Heise Online, October 10, 2007 available online: <http://www.heise.de/english/newsticker/news/97168>



option for potentially achieving the broad safety and security objectives of mass public transit systems.

Underlying much of the information provided by the TTC is the notion that mass transit systems have specific security requirements that give rise to the need for video surveillance. Since mass public transit often involves the movement of large numbers of passengers in small spaces, the risks to passenger security may be easily distinguished from those in outdoor public spaces.

In addition to security, mass transit systems are also concerned with passenger health and safety, operator safety, and crowd control issues that arise from large numbers of passengers on the system. Accordingly, in considering a threshold to determine whether the use of video surveillance is necessary, I am cognizant of the unique and multifaceted needs of mass transit systems such as the TTC.

The documentation reviewed indicated that there is widespread perception among transit system operators and the general public that video surveillance systems are useful in preventing crime and aiding in criminal justice processes. There is also a growing body of empirical evidence to suggest that video surveillance systems may be an effective part of a crime prevention and national security strategy, aiding in police investigations. In addition, transit system security experts and national security experts continue to strongly recommend the use of video surveillance systems as one component of a comprehensive security strategy for mass transit systems. I have taken all of these factors into consideration in assessing whether or not the TTC has sufficient justification for expanding its use of video surveillance.

In my view, safety and security are essential components to the proper functioning of the Toronto public transit system. In order to preserve the safety and security of the system, the TTC must address not only the growing issues of operator assaults, crime on the TTC, and the potential threat of terrorism, but especially the challenge of moving hundreds of thousands of passengers safely and quickly, on a daily basis. Given the nature of the safety and security needs and the massive scope and complexity of the public transit system in the City of Toronto, achieving these goals through a combination of other measures (e.g., increased security personnel, enhanced lighting) would not be feasible. The best strategy would be to employ the full range of safety and security options available, which would include video surveillance.

Finally, to return to the test expressed by the Ontario Court of Appeal in *Cash Converters*, in order for a given collection of personal information to satisfy the necessity condition:

... the institution in question must demonstrate that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not “necessary” within the meaning of the *Act*.

In this case, the sole class of personal information at issue is the images of individuals that are passengers on the TTC system. Based on the foregoing, I am satisfied that the collection of individuals’ images is not merely helpful, but is necessary to the proper administration of the TTC. Accordingly, I am satisfied that the collection of personal information through the use of

video surveillance cameras meets the necessity condition, and is therefore in compliance with section 28(2) of the *Act*.

*Used for the Purposes of Law Enforcement (Law Enforcement Condition)*

Although I have concluded that the TTC’s collection of personal information through video surveillance satisfies the necessity condition (i.e., that it is necessary to the proper administration of a lawfully authorized activity), and is therefore permissible under section 28(2) of the *Act*, I will now proceed to consider whether the collection would also be upheld under the law enforcement condition (i.e., that it is used for the purposes of law enforcement).

The TTC has stated that the images collected through its video surveillance system are used for the purposes of law enforcement, and has made reference to the activities of staff working in the TTC’s Special Constable Services Department, who are the primary users of the recorded images collected through the surveillance system.

The definition of “law enforcement” is contained in section 2(1) of the *Act*, which states:

“law enforcement” means,

- (a) policing,
- (b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
- (c) the conduct of proceedings referred to in clause (b);

With respect to the role of staff working in Special Constables Services Department, the TTC has stated:

... the employees within our Special Constable Services Department have been granted “special constable” status by the Toronto Police Services Board and the Solicitor General. As such, special constables have been conferred the powers of a police officer for specific purposes, including enforcing the Criminal Code throughout the transit system.

The TTC’s description of the powers of a “Special Constable” are supported by section 53 of the *Police Services Act*, which states, in part:

- (1) With the Solicitor General’s approval, a board may appoint a special constable to act for the period, area and purpose that the board considers expedient.

...

- (3) The appointment of a special constable may confer on him or her the powers of a police officer, to the extent and for the specific purpose set out in the appointment.

...

In addition to the *Police Services Act*, further details about the status of TTC Special Constables may be found in a May 9, 1997 Agreement (as amended) between the Toronto Police Services Board (the Board) and the TTC, which sets out the powers, jurisdiction and certain procedures of the TTC Special Constables.

TTC Special Constables may enforce various federal and provincial statutes, including the federal *Criminal Code* and related drug and controlled substances legislation, the provincial *Mental Health Act*, *Trespass to Property Act*, *Liquor Licence Act* and specified sections of the *Provincial Offences Act*. In addition, TTC Special Constables may enforce TTC By-Law #1, which sets out the rules that passengers are required to follow to promote, among other goals, public safety and security. For example, the by-law provides that:

No person shall commit any nuisance, disturb the peace, or act contrary to public order, in or upon any vehicle or premises of the Commission.

No person shall carry, nor shall the Commission be required to carry on any vehicle, any goods which are of an offensive, dangerous, toxic, flammable or explosive nature that are likely to alarm, inconvenience, cause discomfort, or injure any person, or cause damage to property, whether or not such goods are contained in an approved container, without authorization.

The jurisdiction of the TTC Special Constables is subject to geographic restriction. TTC Special Constables' jurisdiction is limited to properties and vehicles under TTC control, and all facilities and leased/rented properties affiliated or associated with the TTC, within the City of Toronto. Additionally, if an offence originates on, or is in relation to, TTC property, a TTC Special Constable may investigate such offence within the City of Toronto.

The Agreement also sets out procedures relating to the investigative authority in certain situations and with respect to certain offences between the Police and TTC Special Constables. For example, if a Police officer and a TTC Special Constable both attend a call within the geographic jurisdiction of the TTC, or if a dual procedure or indictable offence is involved (i.e., those offences of a more serious nature), TTC Special Constables must take instruction and direction from Police. If the alleged offence is not a dual procedure or indictable offence, the TTC Special Constables shall proceed to conduct the investigation. The Agreement further provides that the Police have primary responsibility for responding to and investigating serious occurrences on the transit system (e.g. violence involving weapons, violent incidents where injury has occurred or is likely to occur), while TTC Special Constables may respond to minor physical assaults not involving weapons or verbal confrontations. Finally, the Agreement provides that, for a specified list of offences that includes robbery, weapons, drugs, explosives and sexual offences amongst others,

the Police must be called and may investigate. The Police need not be called, however, where the alleged offence involves theft under \$5000.

The Agreement provides that the TTC Special Constables shall be trained by the TTC in accordance with training standards prescribed by the Board for members of the Police, as modified for the TTC Special Constables considering their powers, duties and responsibilities.

Other factors which I find relevant include the following: TTC Special Constables may have access to confidential police information, such as CPIC and criminal record information; TTC Special Constables, although prohibited from carrying weapons and carrying out vehicle pursuits, may carry “pepper spray;” TTC Special Constables may make arrests and must transfer persons detained in custody to police; every arrest and investigation of a criminal offence conducted by a TTC Special Constable must be reported to the Police.

Finally, the TTC must establish a complaints investigation procedure regarding the conduct of TTC Constables that corresponds to that of the Police, and must provide the Board with the results of all complaints investigations, as well as any information concerning misconduct or alleged misconduct. The Board may, if provided with a finding of misconduct or information regarding misconduct, suspend or terminate the appointment of a TTC Special Constable.

Considering the foregoing, and in particular the authority under section 53 of the *Police Services Act* and the powers, jurisdiction and procedures set out in the Agreement between the TTC and the Board, I am satisfied that the TTC Special Constables engage in “policing” and thus meet the definition of “law enforcement” under the *Act*. Although in certain contexts, the status and authority of the TTC Special Constables may be construed as subordinate to that of the Police, I nevertheless find that their activities are sufficiently similar to the Police such that they come within the meaning of “policing” under the “law enforcement” definition.

Finally, I am satisfied that when the video surveillance system is accessed on an incident-driven basis to pursue an investigation by the TTC Special Constables it is “used for the purposes of law enforcement” and the underlying collection is therefore in compliance with the law enforcement condition of section 28(2).

### *Section 28(2) – Conclusion*

I note that a given collection of personal information is permissible under the *Act* where it may be justified under at least one of the section 28(2) conditions. Based on the foregoing, I am satisfied that the collection of personal information through the video surveillance system is permitted under two of the section 28(2) conditions. The general collection is satisfied by the necessity condition, as well as the law enforcement condition with respect to the activities of the TTC Special Constables.

Having reached the conclusion that the collection of personal information through the use of video surveillance is permissible under section 28(2) of the *Act*, it is incumbent upon the TTC to govern its video surveillance system in a manner that places a high regard on the privacy of its passengers. While TTC passengers may accept a certain degree of surveillance, they should

not expect that their images or personal information will be improperly recorded or misused for purposes that are secondary to the purposes of safety and security. Therefore, for the remainder of this Report, I will focus on the governance aspects relating to the TTC's use of video surveillance cameras.

**Conclusion:** The collection of personal information by the TTC's video surveillance cameras is in compliance with section 28(2) of the *Act*.

**Issue C: Is the Notice of Collection provided to passengers in accordance with section 29(2) of the Act.**

Section 29(2) of the *Act* states:

If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,

- (a) the legal authority for the collection;
- (b) the principal purpose or purposes for which the personal information is intended to be used; and
- (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

This section requires that institutions collecting personal information provide individuals with the Notice of Collection that is prescribed in section 29(2) of the *Act*. In the case of video surveillance programs, the *Guidelines* elaborate on the statutory requirement to provide a Notice of Collection and state:

The public should be notified, using clearly written signs, prominently displayed at the perimeter of the video surveillance areas, of video surveillance equipment locations, so the public has reasonable and adequate warning that surveillance is, or may be in operation before entering any area under video surveillance. Signs at the perimeter of the surveillance areas should identify someone who can answer questions about the video surveillance system, and can include an address, telephone number, or website for contact purposes.<sup>43</sup>

The *Guidelines* further state that while signs should contain the basic information relaying that individuals are under surveillance, the remainder of the notice requirement may be satisfied by having the entire notice appear in other media, such as in pamphlets and other printed materials.

With respect to the TTC's video surveillance program, the TTC's Policy contains the requirement that, "The TTC shall post signs, visible to members of the public, at all entrances and/or

---

43 See *Guidelines*, page 7.

prominently displayed on the perimeter of the location being video recorded.” The Policy further states that the notice provided on the signs must contain the full notice requirement as set out in section 29(2) of the *Act*.

An appendix to the TTC’s Policy contains an illustration of the signs, which include a picture of a camera and the following text:

This area is being Video Recorded for Security Purposes.

The personal information collected by the use of video equipment at this location is collected under the authority of the City of Toronto Act, 2006 and the *Occupiers’ Liability Act*.

Any questions about this collection can be directed to the Coordinator, Freedom of Information/Records Management, at [phone number and contact information].

With respect to surface vehicles, the TTC has stated that a Notice of Collection decal containing the above wording has been posted on all vehicles in which cameras have been installed. With respect to the subway system, the TTC has acknowledged that signage containing the above wording has not yet been installed, but that plans are underway to install a total of 761 signs throughout the 69 stations. The TTC plans to install the signs as the use of video surveillance cameras expands.

I am satisfied that the Notice of Collection, as drafted, meets the requirements set out in section 29(2) of the *Act* and the *Guidelines*. I am also satisfied that the TTC’s plans with respect to the number and placement of signs are appropriate. However, it is imperative that the TTC ensure that signs are installed prior to the video surveillance cameras being activated at a particular site and I will recommend that my office be advised of such developments.

**Conclusion:** The Notice of Collection provided to TTC passengers is in compliance with section 29(2) of the *Act*.

#### **Issue D: Is the disclosure of personal information to the Toronto Police Service in accordance with section 32 of the *Act*?**

The TTC has acknowledged that recorded video surveillance images collected from both surface vehicles and the subway system are disclosed to the Toronto Police Service (the Police) in response to requests for information about incidents involving criminal investigations. In addition, the TTC has stated that, in the future, the Police will have the ability to remotely access video surveillance images obtained from some of the cameras in the subway system, in accordance with the MOU to be signed. The TTC provided a copy of the draft MOU to my office and indicated that the MOU would be signed once it is passed by the Toronto Police Services Board. This remote access by the Police also constitutes a disclosure of personal information on the part of the TTC, under the *Act*.

The rules relating to the disclosure of personal information are set out in section 32 of the *Act*, which states, in part:

An institution shall not disclose personal information in its custody or under its control except,

- (a) in accordance with Part I;
- (b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
- (c) for the purpose for which it was obtained or compiled or for a consistent purpose;

...

- (g) if disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

...

Section 32 establishes a basic prohibition on the disclosure of personal information, but states that there are certain circumstances under which the disclosure of personal information is permissible. In order for a given disclosure of personal information to be allowed under the *Act*, the institution in question must demonstrate that the disclosure in question is in accordance with at least one of the statutory exceptions set out in section 32. The TTC has cited various section 32 provisions to support its position that the disclosure to the Police is permissible.

In this case, there are generally two different types of disclosures of personal information taking place. The first is the physical disclosure of personal information to the Police (or another law enforcement agency) in response to an incident which may lead to criminal charges. The second type of disclosure is that which results from the direct remote access to video surveillance images of the TTC subway system by the Police.

With respect to the first type of disclosure, the physical disclosure of recorded video surveillance images to law enforcement officials in response to a specific incident, I note that these images may be taken from cameras located in both the subway system and on surface vehicles (including streetcars, once installed).

The TTC's Policy describes the manner in which recorded images collected from the video surveillance cameras in both surface vehicles and the subway system are provided to law enforcement officials, in response to a specific incident:

If access to a video recording record is required for the purpose of a law enforcement investigation, the requesting Officer (or in emergency situations, the Operator that authorized the release) must complete the TTC's Law Enforcement Officer Request

Form ... and forward this form to the [Designated Departmental Management Staff] or designate [who] will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Officer.

In my view, this type of disclosure of personal information, in response to a specific incident, where the requesting officer completes the prescribed form indicating a specific date, time and location of the incident being investigated, would constitute a “disclosure to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result,” within the meaning of section 32(g) of the *Act*. Accordingly, I am satisfied that such disclosures are permissible under the *Act*.

The second type of disclosure (based on direct remote access to video surveillance images by the Police) is the subject of an MOU that has been drafted, but yet to be signed between the Toronto Police Services Board and the TTC. The draft MOU specifies that remote access to the video surveillance images shall only be permitted for law enforcement or public safety purposes and that no other uses are permitted without the express written consent of the TTC. The TTC stated that the remote access would take place from a computer, located within Police headquarters, connected to the TTC’s subway system through a fibre-optic cable. Access to the video surveillance images will be incident-driven, requiring a case file number. Access will also be restricted to only eight designated individuals, within the Video Services Unit.

The initial draft of the MOU provided to my office indicated that the Police would have remote access to both live and recorded video surveillance images. My office was concerned that access to the live video surveillance feed by the Police could lead to potentially invasive activities and improper surveillance. During the course of the investigation, the TTC revised the draft MOU to restrict the Police’s remote access to recorded images only. Since the recorded images are only retained for a short period of time, I have less concern with this type of disclosure to the Police.

However, to ensure that each disclosure of personal information to the Police is for legitimate law enforcement and public safety purposes, all disclosures of personal information must be subject to stringent accountability and oversight. Accordingly, I recommend that prior to providing the Police with direct remote access to the recorded video surveillance images, the TTC should amend the draft MOU to require that the logs of disclosures to the Police be subjected to regular audits, conducted on behalf of the TTC. The TTC should provide my office with a copy of the revised draft MOU prior to signing.

**Conclusion:** The disclosure of personal information to the Toronto Police Services is in compliance with section 32 of the *Act*.

**Issue E: Does the TTC have adequate security measures in place to safeguard the personal information collected?**

Regulation 823, made pursuant to the *Act*, addresses the general security requirements for records in the custody of an institution. Section 3 of Regulation 823 states:



- (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.
- (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
- (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

The *Guidelines* elaborate on the security responsibilities of institutions operating video surveillance systems and state, in part:

- All tapes or other storage devices that are not in use should be stored securely in a locked receptacle located in a controlled-access area. Each storage device that has been used should be dated and labeled with a unique, sequential number or other verifiable symbol.
- Access to the storage devices should only be made by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail. Electronic logs should be kept where records are maintained electronically.<sup>44</sup>

Under the section dealing with an institution’s video surveillance policy, the *Guidelines* state:

Employees should be subject to discipline if they breach the policy or the provisions of the *Acts* or other relevant statutes. Where a service provider fails to comply with the policy or the provisions of the *Act*, it would be considered a breach of contract leading to penalties up to, and including, contract termination.

Employees of institutions and employees of service providers should sign written agreements regarding their duties under the policy and the *Acts*, including an undertaking of confidentiality.<sup>45</sup>

Privacy International stated that there has been “insufficient consideration regarding access powers” on the part of the TTC. My office understood this comment to mean that Privacy International is of the view that, in implementing its video surveillance cameras, the TTC did not incorporate sufficient controls over who would have access to the live and recorded video surveillance images. With due respect, I disagree with this assertion. In materials provided to my office, the TTC described the security measures put in place to prevent unauthorized access to the images obtained through the video surveillance system.

---

44 See *Guidelines*, page 8.

45 See *Guidelines*, page 5.

With respect to the cameras located in TTC surface vehicles, the TTC noted that the hard drives containing the recorded video images are only accessible through the use of a password, which is only available to a limited number of TTC supervisors. The operators of TTC vehicles do not have any access to the recorded video images. The TTC stated:

In order to access, view and/or record extracted data a separate computer is required and can only be performed by authorized TTC personnel. To remove a recorder from a vehicle requires a special tool key, which is not available to operators. ... In addition, if a camera is moved, altered or in any way tampered with, the recorder creates an internal log indicating the occurrence and the time.

The TTC also provided a copy of a document entitled, *Interim TTC Protocol for Surface Vehicle Safety Camera System*, which documents the manner in which access may be granted to the recorded images collected by cameras located in surface vehicles in response to specific investigations.

The TTC has similar measures in place relating to the cameras located on the subway system. The TTC provided my office with a copy of written procedures describing the TTC's internal process for requesting images recorded at a given site within the subway system. These procedures describe the way in which recorded images may be used internally, the staff designations who may have access to them, and the manner in which access may be provided. The TTC also noted that all designated staff permitted access to recorded images must receive training on privacy and security:

All TTC personnel that access recorded video images are required to log all activities relating to such access, including the time and purpose. A log book is maintained within each station ... [E]ach recorder also creates its own internal log every time the recorder is accessed or an image is accessed.

Further, the TTC has stated:

Cameras located within a specific subway station simultaneously transfer images to a recorder located within a secure room and area of the subway station. All recorders are in a locked cabinet, in a restricted access room.

In my view, the security measures in place, based on the information contained in the TTC's Policy, the written procedures, as well as other information provided, are comprehensive. However, I note that the TTC's Policy does not contain the requirement, as set out in our *Guidelines*, that all employees dealing with the video surveillance system must sign written agreements regarding their duties under the Policy and the *Acts*, including an undertaking of confidentiality. Accordingly, the TTC should amend the Policy to incorporate such wording to fully satisfy its responsibilities relating to security of recorded information under Regulation 823 and the *Guidelines*.

**Conclusion:** The TTC has adequate security measures in place to safeguard the personal information collected. However, the TTC should amend its Policy to require that all employees

dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.

**Issue F: Does the TTC have proper destruction processes in place for recorded information that is no longer in use?**

As discussed above, Regulation 823 requires that institutions have proper security safeguards in place to protect records from unauthorized access. The principle that unauthorized access should be prevented applies to all aspects of a record's life cycle, up to, and including, its destruction.

The *Guidelines* address the destruction of records that have been created through the use of video surveillance in the past and state:

Old storage devices must be securely destroyed in such a way that the personal information cannot be reconstructed or retrieved. Destruction methods could include overwriting electronic records, shredding, burning or magnetically erasing the personal information.<sup>46</sup>

In sum, the *Guidelines* recommend the secure destruction of all recorded video images.

With respect to the images collected from surface vehicles, the TTC stated that the system is designed to automatically overwrite every 15 hours. Since actual recording only takes place when the vehicle is in operation, the images will be deleted and overwritten with new images at least every 24 hours.

The TTC's Policy addresses the secure destruction of video records, and states:

The TTC will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal. Old storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.

In addition to the general destruction requirements expressed in the Policy, the TTC has also provided specific information on the secure destruction of recorded images. With respect to images taken from recorders located on surface vehicles, the TTC stated:

If a request for images is received, the images are downloaded from the digital video recorder to an investigation station (laptop computer). If the images are to be retained, the images are burned from a laptop computer to a DVD. All laptop computers which contain appropriate software to download video recorded information from vehicles are equipped with a file shredding application

---

<sup>46</sup> See *Guidelines*, page 9.

which shreds each downloaded file upon being activated by the authorized TTC supervisor.

With respect to the images recorded from the subway system, the TTC stated that images are retained in a controlled-access area of any given subway station. Images are retained for a maximum retention period of seven days, and then overwritten.

In light of the information provided by the TTC, I am satisfied that the destruction methods for images retained from video surveillance cameras are appropriate and in compliance with the requirements under our *Guidelines*. I am also satisfied that these destruction methods constitute “reasonable measures” to protect the security of recorded images under section 3 of Regulation 823.

**Conclusion:** The TTC has proper destruction processes in place for recorded information that is no longer in use.

### **Issue G: Does the TTC have proper retention periods in place for personal information that is collected?**

Section 5 of Regulation 823 establishes a minimum retention period for personal information that has been collected by an institution, and states:

Personal information that has been used by an institution shall be retained by the institution for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, unless the individual to whom the information relates consents to its earlier disposal.

This provision establishes a minimum one-year retention period for personal information that has been “used.” The purpose of this provision is to require that institutions maintain records containing personal information for at least one year in order to facilitate a right of access by individuals to their own personal information.

I note that the one-year retention requirements for records that **have been used** are not currently expressed in the Policy or in materials provided to my office. Accordingly, I will be recommending that the TTC incorporate the appropriate retention periods into the Policy before it is finalized.

The *Guidelines* elaborate on the retention requirement in the Regulation and recommend a retention period for video surveillance images that have been collected but **have not been used**, and state:

- The organization should develop written policies on the use and retention of recorded information that:

...

- Set out the retention period for information that has not been viewed for law enforcement or public safety purposes. Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule (normally between 48 and 72 hours).

...

- Establish a separate retention period when recorded information has been viewed for law enforcement or public safety purposes.<sup>47</sup>

...

In the Policy, the TTC has not finalized the retention period for recorded images collected from video surveillance cameras. However, in materials provided to my office, and addressed above, the TTC has stated that images recorded from surface vehicles would be overwritten after 15 hours if the image had not been used as part of an investigation. For the subway system, images will be overwritten after a period of seven days, if not used.

The TTC has provided my office with Transport Canada’s *Closed Circuit Television Reference Manual for Security Applications*, which recommends retention periods of between seven and 30 days for images recorded from video surveillance cameras. My office’s *Guidelines* recommend a shorter retention period of 72 hours. Video surveillance cameras operated by the Police in the entertainment district of downtown Toronto currently operate successfully with a maximum retention period of 72 hours and have operated on this basis for several years. In my view, 72 hours provides a sufficient window of time for the TTC and the Police to determine if an incident has occurred and if video surveillance footage may be relevant to its investigation. Therefore, I see no reason to extend the retention period beyond the recommended 72 hours.

**Conclusion:** The TTC should amend its retention periods for video surveillance images that have not been used from the current maximum of seven days to a maximum of 72 hours.

**Issue H: Has the TTC undertaken all appropriate steps prior to implementing video surveillance?**

With respect to Privacy International’s assertion that the “scheme is being deployed without consideration of privacy and associated protocols,” I note that the TTC’s draft Policy has actually been modeled on the recommended provisions outlined in my office’s *Guidelines for the Use of Video Surveillance Cameras in Public Places*, which are intended to provide direction on the deployment of video surveillance in a privacy-protective manner. The TTC has been careful to ensure that the key privacy provisions of the *Guidelines* have been incorporated into their draft Policy.

Our *Guidelines* provide recommendations regarding the steps that institutions should take prior to engaging in video surveillance.

---

47 See *Guidelines*, page 8.

The *Guidelines* state, in part:

- An assessment of privacy implications should be conducted on the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated by examining the collection, use, disclosure and retention of personal information.

...

- Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public. Extensive public consultation should take place.<sup>48</sup>

...

As discussed above, the TTC has engaged in public consultation on certain elements of its video surveillance system. For instance, the TTC has sought the public's opinion on the design of new streetcars, and invited the public to provide comment on mock-ups of the new subway cars. In both cases, the presence of video surveillance cameras was considered to be positive by those involved in the consultation process.

With respect to the requirement that the TTC conduct a formal assessment into privacy impacts, the TTC noted that, as an Appendix, the Policy contains a *Surveillance Video Security Threat Assessment*. The TTC noted that a formal threat assessment will be completed prior to the finalization of its Policy, which is planned for early 2008.

The IPC *Guidelines* recommend “extensive” public consultation to ensure that stakeholders are educated and informed of the video surveillance system and given an opportunity to provide feedback. While the TTC has undertaken some consultations, these consultations were not specific to the TTC's overall video surveillance program. I am not convinced that these consultations fulfill the requirements of our *Guidelines* and have concluded that the steps taken prior to the implementation of video surveillance by the TTC, specifically with respect to extensive public consultation, are not sufficient.

As the TTC continues to expand its video surveillance program, I recommend that more public consultations take place, possibly in the form of town hall meetings, to broadly educate the public and publicize the expansion of the video surveillance system in Toronto's public transit system. In addition to conducting public consultations, I recommend that the TTC inform the public of its video surveillance program by publishing general information on its website and in printed materials, as appropriate.

**Conclusion:** As the TTC expands the use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.

---

48 See *Guidelines*, page 4.

## Issue I: Is the TTC's video surveillance system subject to regular audits?

In the context of video surveillance, an audit should be viewed as a thorough examination of an institution's policies, practices and procedures as well as a test of internal compliance with the obligations set out under these documents. The audit requirement is expressed in our *Guidelines* as follows:

Organizations should ensure that the use and security of video surveillance equipment is subject to regular audits. The audit should also address the organization's compliance with the operational policies and procedures. An external body may be retained in order to perform the audit. Any deficiencies or concerns identified by the audit must be addressed immediately.

Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.<sup>49</sup>

The general utility of organizational privacy audits has been recognized by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA), who have jointly published their *Generally Accepted Privacy Principles (GAPP) – A Global Privacy Framework* (the *GAPP Privacy Framework*).<sup>50</sup> The *GAPP Privacy Framework* was developed to assist organizations in identifying and managing privacy risks and serves as an excellent basis for conducting independent audits.

The TTC has developed comprehensive policies and procedures that seek to minimize improper access and intrusions into the privacy of individuals. The systems described above, which contemplate defined staff privileges and a paper trail of access documented through logs, are also intended to prevent potential abuses of their surveillance system.

Notwithstanding these protections, the size and complexity of the TTC as an organization, as well as the extent of surveillance due to the number of cameras in operation, gives rise to the potential for abuse. Accordingly, regular system-wide audits (at least on an annual basis) will help to ensure that the system is operating properly with respect to privacy and will help to reduce the risk of a privacy breach.

In the materials provided to the IPC, the TTC made reference to plans for conducting annual audits of their surveillance system. In the Policy, under the section "Roles and Responsibilities," the General Secretary of the TTC is listed as being responsible for ensuring Policy compliance and for coordinating annual audits of the TTC's video surveillance system.

The TTC's Policy provides no further elaboration of these audits. There is no separate heading for audits in the Policy nor is there any reference to the requirement that audits be conducted on an annual basis.

---

49 See *Guidelines*, page 10.

50 The *GAPP Framework* is available from the CICA's website: [http://www.cica.ca/index.cfm/ci\\_id/36529/la\\_id/1](http://www.cica.ca/index.cfm/ci_id/36529/la_id/1).

Accordingly, I am recommending that the TTC amend its Policy in order to make the audit requirement more explicit. I am also recommending that the TTC provide a copy of its first annual audit to the IPC's Policy Department for review. Review by my office will help to ensure that the audit is methodologically sound and comprehensive in its scope. In addition, the initial audit should be performed by an independent third party using the *GAPP Privacy Framework* and should also assess the TTC's compliance with the recommendations made in this Report. This will allow my office to follow up on any shortcomings identified through the audit.

**Conclusion:** The TTC must ensure that its video surveillance program is subjected to an effective and thorough audit conducted by an independent third party, using the *GAPP Privacy Framework*.

## Summary of Conclusions

In summary, I have made the following conclusions in this investigation:

- A. The information collected by the TTC's video surveillance cameras qualifies as "personal information" as defined under section 2(1) of the *Act*.
- B. The collection of personal information by the TTC's video surveillance cameras is in compliance with section 28(2) of the *Act*.
- C. The Notice of Collection is provided to TTC passengers in compliance with section 29(2) of the *Act*.
- D. The disclosure of personal information to the Toronto Police Services is in compliance with section 32 of the *Act*.
- E. The TTC has adequate security measures in place to safeguard the personal information collected. However, the TTC should amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.
- F. The TTC has proper destruction processes in place for recorded information that is no longer in use.
- G. The TTC should amend its retention periods for video surveillance images that have not been used from the current maximum of seven days to a maximum of 72 hours.
- H. As the TTC expands its use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.
- I. The TTC must ensure that its video surveillance program is subjected to an effective and thorough audit conducted by an independent third party, using the *GAPP Privacy Framework*.



## Recommendations

In light of the conclusions contained in this Report, I recommend that the TTC take the following steps to enhance the protection of personal information collected through its video surveillance system. Specifically, I make the following recommendations:

1. That, prior to providing the Police with direct remote access to the video surveillance images, the TTC should amend the draft MOU to require that the logs of disclosures be subjected to regular audits, conducted on behalf of the TTC. A copy of the revised draft MOU should be provided to my office prior to signing.
2. That the TTC amend its Policy to reflect the conditions set out in the revised MOU.
3. That the TTC amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.
4. That the TTC advise my office of its progress in installing the signs providing Notice of Collection to passengers.
5. That the TTC amend its retention periods for video surveillance images from a maximum of seven days to a maximum of 72 hours.
6. That the TTC amend its Policy to include applicable retention periods, both for when images are used (minimum of one year) and when the images are not used (either 15 hours or 72 hours, depending on where the camera is situated).
7. As the TTC expands its use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.
8. That the TTC include an additional heading in its Policy specifically addressing the annual audit requirement. The Policy should state that the annual audit must be thorough, comprehensive, and must test all program areas of the TTC employing video surveillance to ensure compliance with the Policy and the written procedures. The initial audit should be conducted by an independent third party, using the *GAPP Privacy Framework*, and should include an assessment of the extent to which the TTC has complied with the recommendations made in this Report.
9. That the TTC provide my office with a copy its first annual audit for review, and comment on the details and methodology of the audit.
10. That the TTC provide my office with a copy of its revised Policy no later than one month after the date of this Report.
11. That the TTC should keep abreast of research on emerging privacy-enhancing technologies and adopt these technologies, whenever possible.
12. That the TTC should select a location to evaluate the privacy-enhancing video surveillance technology developed by the University of Toronto researchers, K. Martin and K. Plataniotis.
13. Within three months of the date of this Report, the TTC should provide my office with proof of compliance or an update on the status of its compliance with each of these recommendations.

## Commissioner's Message

The area of video surveillance presents a difficult subject matter for privacy officials to grapple with impartially because, on its face, it is inherently privacy-invasive, due to the potential for data capture. Despite that fact, there are legitimate uses for video surveillance, as outlined in this Report, that render it in compliance with our privacy laws. The challenge we thus face is to reign in, as tightly as possible, any potential for the unauthorized deployment of the system. We have attempted to do this by ensuring that strong controls are in place with respect to its governance (policy/procedures), oversight (independent audit, reportable to my office) and, the most promising long-term measure, the introduction of innovative privacy-enhancing technologies to effectively eliminate unauthorized access or use of any personal information obtained.

In light of the growth of surveillance technologies, not to mention the proliferation of biometrics and sensing devices, the future of privacy may well lie in ensuring that the necessary protections are built right into their design. "Privacy by design" may be our ultimate protection in the future, promising a positive-sum paradigm instead of the unlikely obliteration of a given technology. My goal is to have privacy embedded into the architecture of all future technologies, thereby preserving it well into the future.



Ann Cavoukian, Ph.D.  
Commissioner

March 3, 2008

---

Date

**Appendix H:**

Transcript of the Office of the Privacy  
Commissioner's Appearance  
before the House of Commons Standing  
Committee on Access to Information, Privacy and  
Ethics (ETHI) on the Privacy Implications of  
Camera Surveillance, October 22, 2009,  
Ottawa, Ontario

## Office of the Privacy Commissioner of Canada

This page has been archived.

---

### Appearances before Parliamentary Committees

## **ARCHIVED - Appearance before the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Privacy Implications of Camera Surveillance**

October 22, 2009  
Ottawa, Ontario

Statement by Elizabeth Denham  
Assistant Privacy Commissioner of Canada

(Check against delivery)

---

Thank you, Mr. Chairman and members of the Committee for inviting our Office to address you on the privacy implications of camera surveillance, as used in such commercial applications as Google Street View and Canpages and other issues related to video surveillance and new technology. I am joined today by my colleagues, Carman Baggaley, our senior strategic policy advisor, and Daniel Caron, Legal Counsel. Unfortunately Commissioner Stoddart cannot attend today. She has laryngitis. I think this is a first for her not attending.

We very much appreciate the Committee's interest in this issue and we followed the hearing on June 17, 2009, at which representatives from Google and Canpages appeared. We welcome the opportunity to discuss this interesting development in technology.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is a technology neutral law that does not, in our view, thwart the innovation of new technologies. We have sought to ensure that PIPEDA is a dynamic, modern and effective tool to strengthen the privacy rights of Canadians, and we believe that PIPEDA can cope with the commercial collection and use of personal information through street-level imaging technology.

We are very much aware that many services that use street-level imaging are popular with the public. Our ongoing concerns about the commercial use of this technology centre on ensuring that it protects the privacy of Canadians by meeting the requirements of PIPEDA, such as knowledge and consent, safeguards and retention.

I would like to now briefly recap our involvement in this issue.

### **Background**

The Office of the Privacy Commissioner of Canada has been closely following the development and use of on-line street-level imaging technology by companies operating in Canada and elsewhere for a few years. As I indicated, such technology has potential privacy concerns and we wanted to know more about it and how it may be deployed in Canada.

Street-level imaging applications use various means of photographing the streetscape. A camera is typically mounted on a vehicle that is driven down a street. The images are then shown on the internet as part of the company's mapping application. Although the companies' interest is to capture a streetscape so that users can take a virtual tour of a particular neighbourhood, the companies are also capturing images of identifiable individuals and tying them to specific locations.

We began to monitor this issue in 2007, when we learned that Google was photographing the streets of certain Canadian cities for the eventual launch of its Street View application in Canada, without the apparent knowledge or consent of the individuals who appeared in the images.

The Commissioner wrote an open letter to Google, outlining my concerns about the Street View application. She took the opportunity to point out that if companies like Google wished to use this technology for commercial services in Canada, there was private-sector privacy law that would have to be adhered to and stronger privacy protections would have to be put into place.

## Photographing people in public places

I would like to address a common misconception that some companies have about photographing people in public places. If an organization takes a photograph of an individual in a public place for a commercial purpose – for example, when a company, in the course of photographing a streetscape captures an identifiable image of a person and the image is uploaded onto the internet, for a commercial reason – Canadian privacy law still applies. One of the key protections is that people should know when their picture is being taken for commercial reasons and what the image will be used for. Their consent is also needed. While there are exceptions under the law, they are limited and specific and concern journalistic, artistic and literary pursuits.

## Our views on privacy and street-level imaging

Street View has now been launched in Canada — it went live on October 7 — as well as in other countries, and the Canpages service, Street Scene, was launched earlier this year in certain cities in British Columbia. Canpages is seeking to expand its service to other Canadian cities, and has recently provided notice that it is photographing streets in Montreal and Toronto.

Our office and our provincial counterparts with substantially similar commercial privacy laws (Alberta, BC and Quebec) have been in contact with both companies about their street-level imaging and mapping applications. Early this year, those provincial privacy commissioners and our commissioner issued a fact sheet, which I believe you have a copy of, for industry and the public on what we think needs to be in place in order for commercial services that use such technology to be in compliance with Canada's privacy laws. The fact sheet, entitled [Captured on Camera](#), details the privacy protections that are particularly pertinent in the case of street-level imaging. These are:

- Citizens need to know in advance that street-level images are being taken, when, and why, and how they can have their image removed if they don't want it to appear online. This could include visible marking on vehicles — and if you've seen the Google car you'll see that it's well identified; notification through a variety of media outlining dates and locations, the purpose of filming and how people can contact them with questions.
- We also think that faces and license plates need to be blurred so that the individual is made anonymous or is at least not identifiable.
- Companies need an effective and quick take-down process whereby an individual can have their image removed
- Unblurred images retained for legitimate business purposes should be protected with appropriate security measures and the raw data should not be retained indefinitely.

We have seen changes to how the technology is used that are more privacy respectful, and we played an important role in encouraging these changes – not only in Canada but worldwide. Images of people and

licence plates are blurred but the process of doing so needs to continue to evolve and improve. Take-down processes are being established. The need for clear retention periods is being addressed. Companies appear to understand the need to solicit the views of community organizations about any possible sensitivity to filming in certain locations.

Notifying the public is an ongoing concern. We believe that the nature of the information collected is not especially sensitive and that companies can rely on implied consent provided they give reasonable notification to the public in the form of outreach. Individuals need to know in advance when an organization will be photographing their neighbourhood so that they may adjust their plans accordingly.

## **New technology and PIPEDA**

As you know, the purpose of PIPEDA is to balance the individual's right of privacy with an organization's need to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. PIPEDA applies to a wide range of businesses – from banks and telecommunications companies to car dealerships and the local social networking sites. The law is not prescriptive; rather, it requires organizations to adhere to a set of fair information practices or principles. Each organization, given its business model and other regulatory requirements, must find ways to adhere to these principles and achieve the balance between its own legitimate needs and the rights of individuals to their privacy. The Office of the Privacy Commissioner of Canada works with organizations to help meet their business objectives and meet their obligations under PIPEDA. I'd be very pleased this morning to talk to you about Facebook as a good example of that.

As I indicated earlier, PIPEDA is a technology-neutral and principle-based law and so far appears to be flexible enough to guide commercial uses of new technology. As you are likely aware, over the summer we released findings in two complaints that were filed in 2008, in which new technology and new business models featured prominently. One involved a social networking site, Facebook, and, the other, the use of deep packet inspection (DPI) by a telecommunications company. Under PIPEDA, we were able to strike a reasonable balance that serves as a road map to help us face new privacy challenges on the horizon. These findings will have a positive impact on the privacy rights of Canadians (and indeed on 300 million people worldwide who are users of Facebook), while at the same time acknowledging business interests. What we have learned in the past 18 months, through our work in street-level imaging, social networking sites and deep packet inspection, will help us significantly, and we believe that these examples have served to raise the profile of privacy for business and average Canadians.

As we note in the PIPEDA Annual Report for 2008, new technology, for all its indisputable benefits, continues to pose new privacy challenges. Indeed, our Office is planning to explore, over the next year, the implications of behavioral advertising, cloud computing and geospatial technology on privacy. We will be seeking the views of business, academics, advocates, and regular Canadians in order to better understand how PIPEDA applies to these technologies and business practices and their impact on privacy.

Since we were asked to appear, we tabled our 2008 PIPEDA annual report and I understand that you all have copies. The main themes of the report are really a shout-out to youth, a reminder that Canadians need to take control of their personal information on the Internet. We think that youth are particularly vulnerable because they're big users of technology and may not realize the risks.

Therefore, as our report indicates, we really focused this year on public education activities to reach out and talk to that demographic.

We've passed out some stickers for you, *Think before You Click*. We distributed those during frosh week. We also have many other tools: a youth blog, we have videos produced by youth, so we have youth talking to youth. You can find all of these tools on our website [Youthprivacy.ca](http://Youthprivacy.ca), the federal, provincial and territorial commissioners passed a resolution in 2008 on youth privacy advising what individuals and organizations need to do.

Lastly, before I close, the other main issue I would like to highlight in the annual report is the matter of data breaches and notification. As you know, this is a global issue. Governments, organizations, and data protection commissioners are really grappling with various models including mandatory breach notification.

The report highlights a study that we conducted on our current voluntary reporting regime. I'm happy to talk about it more, but what it confirmed is that we can't possibly be receiving reports from businesses about all significant privacy breaches in Canada. There's just no way. The numbers are relatively low. It underscores also the ongoing need for training because a third of the breaches reported to us were not the result of hacking, of technology breaches, but really simple employee errors like dialing the wrong fax number.

## **Conclusion**

In conclusion, I would like to thank the Committee for inviting us today to discuss privacy, street-level imaging and other new technologies. I welcome your questions.

---

Date Modified: 2009-10-29