

캐나다대법원

서지정보: R. v. Spencer, 2014 SCC 43	날짜: 20140613 사건번호: 34644
----------------------------------	-----------------------------

소송당사자:

항소인 매튜 데이빗 스펜서

과

피항소인 여왕폐하(역사 - 캐나다 정부를 의미함)

그리고

제 3 자 참가인

검찰총장, 온타리오주 검찰총장,

앨버타 검찰총장, 캐나다 프라이버시커미셔너, 캐나다민권협회와 온타리오주
형법변호사협회

판사: McLachlin C.J. and LeBel, Abella, Rothstein, Cromwell, Moldaver,
Karakatsanis and Wagner JJ.

판시이유: 1 문에서 87 문까지	Cromwell J. (McLachlin C.J. and LeBel, Abella, Rothstein, Moldaver, Karakatsanis and Wagner JJ. 별도 의견)
--------------------	---

주석: 이 문서는 캐나다대법원판례집에 포함되기 전까지 수정될 수 있음.

[상기 동일 정보 반복부분 생략]파일번호 : 34644.

2013: December 9; 2014: June 13.

사스카치완 항소법원에서 항소

[색인어 생략]

경찰은, 인터넷 파일 공유 프로그램을 사용해서 아동 포르노에 접근하고 저장한 사람의 컴퓨터의 인터넷 프로토콜 주소(Internet Protocol: 이하 IP 주소)를 확인했다. 경찰은 사법기관의 사전허가 없이 인터넷 사업자로부터 IP 주소와 관련된 망이용계약자의 정보를 획득하였다. 정보요청은 PIPEDA(Personal Information Protection and Electronic Documents Act : 이하 개인정보보호및전자문서법) 7(3)(c.1)(ii)를 염두에 두고 이루어졌고 이를 통해 피고인에게 연결되었다. 피고인은 같은 파일 공유 프로그램을 쓰는 다른 이용자도 접근할 수 있는 폴더에 아동 포르노를 다운받아서, 아동 포르노 소지 혐의에 대해서 유죄 판결과 제공행위에 대한 혐의에 대해서 무죄판결을 받았다. 항소심은 유죄 부분에 대하여 원심판결을 인용하였으나 무죄 부분에 대해서는 재심을 명령하였다.

상고는 기각한다.

프라이버시에 대한 합리적인 기대가 있었는지는 밀접하게 관련된 다수의 요소를 고려하고 검토한 전체적인 상황의 판단에 의해 이루어진다. 이 사건의 쟁점은 수색의 대상과 피고인의 프라이버시에 대한 주관적인 기대가 합리적이었는지 여부이다. 피고인의 프라이버시에 대한 기대의 합리성을 판단할 때는 사안과 관련된 두 가지 요소를 고려해야하는데, 그 요소들이란 처분대상인 프라이버시 이익의 성격과 ISP가 망이용계약자의 정보를 공개하는 것의 계약 및 제정법의 체계이다.

수색의 대상을 살필 때, 법원은 이 사건 정보의 성격뿐만 아니라 그 정보가 노출시키는 정보의 성격에도 주목했다. 이 사건의 경우 수색의 대상은 단순히 ISP와 계약관계에 있는 사람의 이름, 주소가 아니라 특정 인터넷 이용활동과 일치하는 인터넷 이용자의 신원정보이다.

국가의 행위에 관련된 프라이버시법익의 성격은 수색물의 합법성이나 불법성에 달려있는 것이 아니라 목적물에 대한 수색의 영향과 수색물 자체의 프라이버시에 달려있다.

이 사건의 일차적 관심사는 사생활정보의 자기결정권이다. 사생활정보의 자기결정권은 종종 비밀유지나 기밀보장과 동일시되고, 정보에 대한 접근과 이용에 대한 더 넓은 범위의 통제개념을 포함하고 있다. 인터넷 이용의 맥락에 있어서 특히 더 중요한 건 프라이버시를 익명성으로 이해하는 것이다. 이용자의 인터넷활동과 연결된 개인의 신원정보는 정보에 내재된 이름,

주소, 전화번호 이상의 프라이시법익을 발생하게 한다는 점에서 매우 중요하다. 이용자의 신원을 식별케 하는 특정 정보와의 연결고리로서 작용하는 경향이 있는 망이용계약자의 정보는 이를 이용, 소지, 제공하는 개인의 프라이버시법익을 연루시킨다. 일정 수준의 익명성은 인터넷 활동의 특색이며, 상황의 총체성에 기해 익명성은 부당한 압수와 수색으로부터 헌법적으로 보호되는 프라이버시법익의 기초가 된다. 이 사건에서 경찰은 사실상 특정 온라인 활동을 특정 개인과 연결시키기 위해 IP 주소와 대응되는 망이용계약자의 정보를 요청하였다. 이러한 요청은 익명으로 이루어진 온라인 활동(다른 상황에서도 중요한 프라이버시법익을 연계시키는)을 용의자와 연결하기 위한 시도로, 정보프라이버시법익의 익명성 측면을 연계시킨다.

계약 및 제정법적 체계가 관련되어 있다는 것에 이견이 없지 않는 프라이버시의 합리적인 기대 존부를 판단할 때 결정적인 요소는 아니다. 이 사건은 계약 및 제정법적 체계가 겹치고 관련된 조항이 피고인의 프라이버시에 대한 기대의 합리성을 판단하는데 약간의 도움을 줄 뿐이다. 개인정보보호및전자문서법의 7(3)(c.1)(ii)의 적절한 해석은 그 자체가 프라이버시에 대한 합리적인 기대 존부에 기대고 있기 때문에 개인정보보호및전자문서법은 프라이버시의 합리적인 기대 존부에 영향을 주는 요소로 쓰일 수 없다.

인터넷 이용자로서는 경찰의 단순한 요청으로 개인정보를 공개할 의무가 발생한다거나, 동의없이 개인정보를 공개하는 것을 일반적으로 금지하는 개인정보보호및전자문서법에 반하는 행위가 일어나지 않으리라고 기대하는 것이 타당하다. 이 사건의 계약상의 조항은 프라이버시의 합리적인 기대의 존재를 뒷받침한다. 경찰의 요청은, 경찰이 요청만 할 수 있을 뿐 요청을 받아줄 것을 강제할 수 없다는 면에서, 법적 강제력은 없었다. 이 사건의 상황의 총체성의 기해 망이용계약자의 정보에 프라이버시의 합리적인 기대가 있는 것으로 판단된다. 그러므로 ISP가 정보를 자발적으로 공개하게 한 경찰의 요청은 수색에 해당하게 된다.

이 사건 수색의 합법성 여부는 수색이 법에 의해 허용되었는지에 달려있다. 형법 s. 487.014(1)과 개인정보보호및전자문서법은 경찰의 압수, 수색 권한을 인정하고 있지 아니하다. 487.014(1)는 경찰관이 수사할 수 있게 하는 권한의 현존하는 관습법을 확인하는 선언적인 규정이다. 개인정보보호및전자문서법은 개인정보보호를 더 강화하기 위한 목적으로 만들어진 법률이다. 이 사건의 경우, 경찰은 예외적인 상황이나 타당한 법에 의해 망이용계약자의 정보를 수색할 권한이 없으므로, 선언적인 규정과 개인정보를 보호하기 위한 규정의 조합으로 새로운 수색 권한 또한 발생하지 않는다. 이 사건에서 행해진 수색은 권리현장을 위반한다. 경찰의 망이용계약자의 정보 획득 없이는 수색 영장이 발급되지 않았을 것이다. 불법적으로 획득된 그 정보를 판단에서 배제시켰다면 영장을 발급받을 타당한 근거가

결여되었을 것이고 이는 결국 주거를 수색한 것이 불법인 것이고 권리현장을 위반한 것으로 귀결된다.

그러나 경찰은 중요한 수사를 집행할 목적으로 자신의 판단으로는 타당하게 행동한 것이고, 이 사건의 경찰의 행위의 성격은 법집행의 신뢰를 떨어뜨리지 않을 것이다. 권리 현장을 침해하는 행위가 권리 현장이 보호하는 피의자의 법익에 끼치는 영향은 증거를 배제할 것을 뒷받침하며, 기소된 혐의는 중한 혐의이다. 사회는 이 사건의 판결과, 사법시스템이 이와 같은 중한 혐의로 기소된 자들을 다루는데 있어서 비난을 받지 않는 것에 높은 관심을 갖고 있다. 이러한 세 요소의 균형을 맞추어 증거로 인정하는 것보다 증거를 배제하는 것이 법집행의 신뢰를 떨어뜨릴 것이므로 증거로 인정하는 것을 인용한다.

s. 163.1(3)에 의해 기소된 피의자가 포르노 자료가 제공되고 있다는 것을 알고 있다는 것에 대해 입증되어야 함에는 이견이 없다. 그러나 피의자가 고의로 적극적인 행위를 통해 자료의 제공성을 촉진할 필요는 없다. 피의자가 고의로 포르노를 타인에게 제공한 것으로 혐의가 성립한 것으로 판단한다. 미필적 고의 여부가 다투어지고 있었고, 재판관이 제공죄의 범의 요건을 충족시키기 위해서는 적극적인 행동이 필요하다고 잘못된 판시를 내렸기 때문에 미필적 고의 여부를 다루지 못하였으므로, 이 혐

결은 재판관의 무죄결정에 영향을 주었을 것으로 여겨진다. 재심명령을 인용한다.

인용된 판례

언급된 판례: *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211; *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246; *R. v. KangBrown*, 2008 SCC 18, [2008] 1 S.C.R. 456; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403; *McInerney v. MacDonald*, [1992] 2 S.C.R. 138; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Wise*, [1992] 1 S.C.R. 527; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *R. v. Collins*, [1987] 1 S.C.R. 265; *R. v. McNeice*, 2010 BCSC 1544 (CanLII); *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Briscoe*, 2010 SCC 13, [2010] 1 S.C.R. 411; *R. v. Graveline*, 2006 SCC 16, [2006] 1 S.C.R. 609.

인용된 법령

Canadian Charter of Rights and Freedoms, ss. 8, 24(2).

Criminal Code, R.S.C. 1985, c. C46, ss. 163.1(3), (4), 487.014.

Freedom of Information and Protection of Privacy Act, S.S. 1990–91, c. F22.01, s. 29(2)(g).

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 3, 5(3), 7, Sch. 1, cl. 4.3.

인용된 저술

Canada. Report of the Task Force established by the Department of Communications/Department of Justice. *Privacy and Computers*. Ottawa: Information Canada, 1972.

Gleicher, Nathaniel. “Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web” (2009), 118 *Yale L.J.* 1945.

Guterman, Melvin. “A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance” (1988), 39 *Syracuse L. Rev.* 647.

Hubbard, Robert W., Peter DeFreitas and Susan Magotiaux. “The Internet — Expectations of Privacy in a New Context” (2002), 45 *Crim. L.Q.* 170.

Hunt, Chris D. L. “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort” (2011), 37 *Queen’s L.J.* 167.

PatonSimpson, Elizabeth. “Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places” (2000), 50 *U.T.L.J.* 305.

Slane, Andrea, and Lisa M. Austin. “What’s in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations” (2011), 57 *Crim. L.Q.* 486.

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1970.

사스카치완 항소법원 판결 (판사 Cameron, Ottenbreit and Caldwell), 2011 SKCA 144, 377 Sask. R. 280, 528 W.A.C. 280, [2012] 4 W.W.R. 425, 283 C.C.C. (3d) 384, [2011] S.J. No. 729 (QL), 2011 CarswellSask 786, (아동포르노

소지죄 유죄판결을 인용하고 아동포르노 제공죄 무죄판결 (판사 Foley, 2009 SKQB 341, 361 Sask. R. 1, [2009] S.J. No. 798 (QL), 2009 CarswellSask 905)을 파기하고 재심을 명령함)에 대한 항소. 항소를 기각함.

항소인 변호인: Aaron A. Fox, Q.C., and Darren Kraushaar

피항소인 변호인: Anthony B. Gerein, .

Ronald C. Reimer and David Schermbrucker, for the intervener the Director of Public Prosecutions.

Susan Magotiaux and Allison Dellandrea, for the intervener the Attorney General of Ontario.

Jolaine Antonio, for the intervener the Attorney General of Alberta.

Mahmud Jamal, Patricia Kosseim, Daniel Caron and Sarah Speevak, for the intervener the Privacy Commissioner of Canada.

Anil K. Kapoor and Lindsay L. Daviau, for the intervener the Canadian Civil Liberties Association.

Jonathan Dawe and Jill R. Presser, for the intervener the Criminal Lawyers' Association of Ontario.

법원의 판결문은 크롬웰 판사에 의해 작성되었다.

I. 서론

[1] 인터넷은 프라이버시에 관해 새롭고 도전적인 문제를 제기하는 하나의 장이다. 본 상고도 그 중의 하나와 관련이 있다.

[2] 경찰은 인터넷 파일 공유 프로그램을 사용해서 아동 포르노에 접근하고 저장한 사람의 컴퓨터의 인터넷 프로토콜 주소(Internet Protocol: 이하 IP 주소)를 확인했다. 경찰은 사법기관의 사전허가 없이 인터넷 사업자로부터 IP 주소와 관련된 망이용계약자의 정보를 획득하였다. 이는 상고인인 스펜서씨에게 이어졌다. 피고인은 같은 파일 공유 프로그램을 쓰는 다른 망이용계약자도 접근할 수 있는 폴더에 아동 포르노를 다운받아서, 아동 포르노 소지 혐의에 대해 유죄 판결과 제공행위 혐의에 대해 무죄판결을 받았다.

[3] 재판에서 피고인은 경찰이 망이용계약자의 정보를 획득한 것이 권리 헌장에 반하는 수색이었으므로 결과적으로 그 증거는 배제되어야 한다고 주장하였다. 또한 피고인은 다른 사람들이 공유폴더에 접근할 수 있다는 것을 몰랐으므로 고의로 폴더에 있던 내용을 제공한 것이 아니라고 주장하였다. 원심은 부당한 수색과 압수로부터 보호받을 피고인의 권리가 침해되지 않았다고 판단했다. “제공행위” 혐의에 대해서는 포르노에 접근하기 위한 “적극적인 촉진”이 있어야 함에도 피고인은 그 요건을 결하였고, 피고인의 폴더에 다른 이용자들이 접근할 수 있다는 것을 몰랐다는 증거를 신뢰하여 범의가 입증되지 않았다. 그러므로 피고인을 소지혐의에 대해 유죄를 인정하였으나 제공행위 혐의에 대해서는 무죄를 선고했다.

[4] 항소심은 원심 판결을 인용하여 아동 포르노 소지 혐의에 대한 유죄를 인정했으며, 망이용계약자의 정보를 획득한 것은 수색이 아니며 수색이었다고 하더라도 합리적인 수색에 해당한다고 판단하였다. 그러나 제공행위에 대한 원심의 판단은 타인의 포르노에의 접근을 적극적으로 촉진한 것의 증명을 요구한 것에 대해 법리의 오해가 있다고 판단하였다. 제공행위의 혐의에 대해 재심을 명령하였다.

[5] 본 상고는 다음과 같은 네가지의 문제를 제기한다.

1. 경찰이 망이용계약자의 정보를 ISP로부터 획득하여 IP 주소와 대조
확인한 것이 수색에 해당하는지

-본 재판부는 수색에 해당한다고 판단한다.

2. 수색에 해당한다면, 그 수색은 법의 허가를 받았는지

-본 재판부는 허가를 받지 않았다고 판단한다.

3. 허가를 받지 않았다면 결과적으로 획득한 증거는 배제되어야 하는
지

-본 재판부는 그 증거는 배제되지 않아야한다고 판단한다.

4. 원심판결에 아동포르노 ‘제공행위’ 혐의에 대한 법리오해가 있었
는지

-원심판결의 법리오해가 있었으므로 본 재판부는 항소심의 판단을 지
지하여 재심을 명령한다.

II. 분석

A. 경찰이 ISP로부터 IP주소에 대응되는 망이용계약자의 정보를 획득한 것이 수색에 해당하는가?

[6] 피고인은 경찰이 ISP인 Shaw 커뮤니케이션으로부터 IP 주소와 연관된 망이용계약자의 정보를 획득한 것이 수색에 해당한다고 주장한다. 피상고인인 검사는 반대의 입장을 취한다. 본 쟁점에 있어서 본 법원은 피고인의 주장에 동의한다. 관련된 사실관계의 요약은 시작으로 법률분석을 하겠다.

(1) 사실관계 및 재판 경위

[7] 피고인은 함께 거주하던 여동생의 이름으로 등록된 명의로 인터넷에 접속했다. 피고인은 파일 공유 프로그램인 LimeWire(이하 이 사건 프로그램)로 아동 포르노를 다운받았다. 이 사건 프로그램은 P2P(Peer-to-peer system) 방식의 파일 공유 프로그램으로 누구든지 다른 사용자의 컴퓨터로부터 자신의 컴퓨터에 파일을 다운받을 수 있다. 이 사건 프로그램은 파일

이 중앙 데이터베이스로 저장되는 것이 아니라 사용자들끼리 직접 파일을 공유하는 시스템이며 음악과 영화를 다운받는데 주로 쓰이고, 성인 포르노와 아동 포르노를 다운받는 데 쓰일 수도 있다. 피고인이 이 사건 프로그램을 사용하면서 경찰의 수사의 대상이 되었으며 결국 이 사건의 쟁점인 수색에 이르게 되었다.

[8] Saskatoon 경찰서의 Darren Parisien 수사관은 공연하게 취득가능한 소프트웨어를 이용하여 아동 포르노를 공유한 사람을 탐색하였다. 수사관은 다른 이용자의 공유폴더에 얼마든지 접근할 수 있었고 이용자와 관련된 두가지 종류의 숫자를 얻어냈다. 이는 특정 시간에 인터넷에 연결된 컴퓨터와 일치하는 IP 주소와 특정 소프트웨어를 쓰는 컴퓨터에 지정되는 GUID(Globally Unique Identifier) 숫자이다. IP 주소는 파일 공유 과정에서 획득했으며 IP 주소의 일반적인 성격이나 Shaw가 망이용계약자에게 제공하는 IP 주소에 대해 기록에 기재된 것은 별로 없다. *R. v. Ward*에 IP 주소간의 차이점에 대한 언급이 있으며, 이 사건의 목적에 따라 본 재판부는 Parisien 수사관이 획득한 IP 주소는 특정 시간의 컴퓨터 활동과 대응된다는 것을 알고 있다.

[9] Parisien 수사관은 아동 포르노를 공유했다고 보이는 컴퓨터의 IP 주소 목록을 작성해 데이터베이스와 비교하여 특정 IP주소와 대응되는 근접 주소를 색출하였다.

[10] Parisien 수사관은 피고인의 컴퓨터가 온라인으로 이 사건 프로그램과 연결되어있을 것이라고 추정하여 보통 이 사건 프로그램 이용자가 접근하는 방식으로 피고인의 공유폴더에 접속하였다. 아동 포르노로 보이는 대규모의 파일들을 발견했지만 정확한 컴퓨터의 위치와 사용자는 알 수 없었다.

[11] 컴퓨터 사용기록으로 장소와 이용자를 알아내기 위해 수사관은 Shaw에게 수사요청서로 특정 IP주소를 사용하는 망이용계약자의 이름, 주소, 전화번호 등의 정보를 요청했다. 요청은 개인정보보호및전자문서법 7(3)(c.1)(ii)에 근거하여 이루어졌고 경찰이 아동 포르노와 인터넷에 적용되는 형법 R.S.C. 1985, c. C-46의 범죄를 조사하고 있다는 것과 진행되고 있는 수사의 일환으로 망이용계약자의 정보를 요구하는 내용을 담고 있다(관련 법률 규정 전문은 부록으로 첨부되어 있음). 경찰은 제출명령이 없었으며, 제출명령 (이 맥락에서 수색영장과 동일) 발부 요청도 하지 않은 상태였다.

[12] Shaw는 경찰의 요청에 따라서 특정 IP주소와 연계된 이름, 주소, 전화번호 등의 정보(명의자인 피고인 여동생의 정보)를 제공했다. 획득한 정보로 경찰은 소외 피고인의 여동생의 주거에 대한 수색영장을 발급받았고 피고인의 컴퓨터를 압수했다. 피고인의 컴퓨터에서 이 사건 프로그램으로 공유한 방대한 양의 아동 포르노 사진과 동영상이 발견되었다.

[13] 피고인은 형법 제163조 제1항 4호에 반하여 아동 포르노를 소지한 혐의와 동조항 3호에 반해 아동 포르노를 인터넷에 유포한 혐의로 기소되었다. 피고인의 공유폴더에서 발견된 사진이 아동 포르노라는 점에는 이견없다.

[14] 피고인은 경찰이 법원의 사전허가없이 획득한 피고인의 주소를 Shaw로부터 취득한 것이 캐나다의 권리 헌장 제8장에 반하는 부당한 수색이므로 그의 컴퓨터에서 발견된 증거는 배제되어야 한다고 주장했다. 원심은 이 주장을 기각했으며 소지혐의에 대해 유죄판결을 내렸다. 항소심도 원심의 수색에 대한 판결을 인용했다.

(2) Shaw에게 한 요청이 수색에 해당하는가?

[15] 권리 헌장 제8장에 의하면 “모든 사람은 부당한 압수와 수색으로부터 보호받을 권리가 있다.” 대법원은 권리 헌장 제8장을 목적론적 해석 방식으로 접근하는 것의 중요성과 그 접근방식이 프라이버시 보호를 개인의 안전, 자기 충족감, 자율성에 더하여 민주주의 사회의 번영의 필요전제조건으로 보는 것의 중요성을 끊임없이 강조해왔다. : *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 156-57; *R. v. Dyment*, [1988] 2 S.C.R. 417, at pp. 427-28; *R. v. Plant*, [1993] 3 S.C.R. 281, at pp. 292-93; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at paras. 12-16; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733, at para. 22.

[16] 첫 번째 쟁점은 권리 헌장 제8장의 부당한 압수수색에 대한 보호가 이 사건에 포함되었는지 여부다. 이는 경찰이 망이용계약자의 신원정보를 IP주소와 대조 확인하기 위해 한 행위가 권리 헌장 제8장의 압수 수색에 해당되는지에 따라 결정되고, 결국 Shaw가 경찰에게 제공한 정보에 대해, 피고인이 전체적인 상황을 고려하여 프라이버시에 대한 합리적인 기대를 갖고 있었는지에 달려있다. 합리적인 기대가 있었다면 신원정보를 획득한 것은 수색에 해당하게 되는 것이다.

[17] 본 재판부는 상황의 총체성에 기한 합리적인 기대의 존재 여부를 여러 관련 요소들을 고려하며 검토하겠다. 이는 프라이버시법익의 성격과 관련된 두가지 요소를 포함하는데, 국가 행위에 의해 관련된 프라이버시법익의 성격과 프라이버시의 기대와 더 직접적인 관계의 요소를 주관적으로, 객관적으로 바라본 것을 말한다. e.g., *Tessling*, at para. 38; *Ward*, at para. 65. 이러한 고려가 ‘상황의 총체성’에 기해서 이루어져야한다는 것은 요소끼리 밀접하게 연관되어 있어 특정 사건의 상황에 적용되어야하고 전체적으로 조망되어야함을 말한다.

[18] 합리적인 기대를 판단하는데 있어서 고려되는 넓은 범위의 다수의 요소들은 분석에 용이하게 크게 4가지 종류로 나눌 수 있다: (1) 소송대상인 수색의 대상 (2) 청구인의 주요쟁점과 관련된 법익 (3) 청구인의 주요쟁점의 프라이버시에 대한 주관적인 기대 (4) 이러한 주관적인 기대가 상황의 총체성에 기해 객관적으로도 합리적인지에 대한 판단: *Tessling*, at para. 32; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 27; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 40. 그러나 이는 전적으로 사실심리에 해당하는 것이 아니다. 프라이버시의 합리적인 기대는 기술적이기보다는 규범적이다: *Tessling*, at para. 42. 그러므로 분석은 사실적인 맥락에 따라 크게 달라질 수 있으며, 필연적으로 “프라이버시보호에 대한 정부의 대응의 장기적인 결과에 관심있는 합리적인 지식인의 독립적인 가치관의 가치판단

으로 가득 차 있다고 볼 수 있다: *Patrick*, at para. 14; see also *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34, and *Ward*, at paras. 81-85.

[19] 본 재판부는 상고의 두 측면에 대해서 짧게 논하겠다. 원심은 이 사건에서 프라이버시의 주관적인 기대가 없다고 판단하였다. 2009 SKQB 341, 361 Sask. R. 1, at para. 18. 그러나 원심이 수색의 대상을 파악하는데 있어서 사실판단에 오류가 있었다. 수색의 범위를 적절하게 이해할 경우, 피고인이 피고인의 민감정보가 네트워크상으로 전송되는 인터넷활동을 한 것으로부터 피고인이 인터넷활동의 프라이버시에 대한 주관적인 기대를 갖고 있었다는 것을 손쉽게 유추할 수 있다: *Cole*, at para. 43. 피고인의 수색에 대한 직접적인 관심 또한 명백하다. 피고인이 ISP와 계약상 당사자는 아니었지만 계약자의 동의하에 인터넷에 접속하였고 피고인은 자신의 주거에서 자기소유의 컴퓨터로 인터넷을 사용했다.

[20] 이 사건의 주 쟁점은 피고인의 프라이버시의 주관적인 기대가 합리적인지 여부와 수색의 대상을 무엇으로 보는지에 달려있다. 피고인의 프라이버시의 기대의 합리성을 결정하기 위해 처분대상인 프라이버시이익의 성격과 ISP가 망이용계약자의 정보를 공개할 수 있게 하는 계약 및 제정법의 체계를 살펴보아야 한다.

[21] 이 사건에서 본 재판부는 우선 수색의 대상을 검토한 후 국가행위에 포함된 프라이버시법익의 성격을 판단하고 계약 및 제정법의 체계를 살펴보겠다. 이 주제들은 명백하고 상호연관되어 있지만, 이렇게 폭넓은 제하에서 분석을 하며 ‘상황의 총체성’을 모두 살펴보면서도 일정한 집중의 효과도 낼 수 있다. {박경신 여기까지만 자세히 봤습니다.}

(a) 수색의 대상

[22] 피고인은 경찰이 Shaw에게 정보를 요청한 것이 권리 헌장 제 8장의 압수수색에 해당하는 국가행위라고 주장하였다. 본 재판부는 연관된 프라이버시법익을 식별하기 위하여 이 사건 요청의 대상이 무엇인지 고려해야한다.

[23] 보통 수색이라고 주장되는 경찰 행위를 정의하는 것은 단순한 문제이나 예외적인 경우도 존재한다. 이 사건은 그 예외적인 경우에 해당하는데, 당사자와 하급법원은 이 쟁점에 대해 판례에 반영된 현저하게 다양한 관점을 제시했다. (예로 Ward에 권위자들의 의견이 제시되어 있음)

[24] 피고인은 소송대상인 수색의 대상은 IP주소와 망공급자로부터 제공된 주소를 대조해 주소의 거주자의 내밀하고 사적인 정보를 노출시키는 핵심적인 신원정보를 얻어낸 것이라고 주장한다. 반면에, 검사는 이 사건 수색으로 공개적으로 접근 가능한 IP주소와 대응되는 이름, 주소, 전화번호를 획득한 것이라고 주장한다.

[25] 이렇게 대립되는 견해는 Saskatchewan 법원의 결정에 반영되었다. 원심은 검사의 견해를 택하여 경찰이 획득한 정보는 포괄적인 정보로써 피고인의 핵심적인 신원정보에 해당하지 않는다고 보았다. Ottenbreit 항소심도 상당부분 검사의 의견에 동의해 이 사건에서 경찰이 획득한 정보는 단순히 특정 IP주소의 계약자의 신원만을 형성한다고 판단하여 이 신원정보가 결과적으로 인터넷에서 식별가능한 개인의 상당수의 활동을 노출시키는 것은 중요한 문제가 아니라고 보았다. : 2011 SKCA 144, 377 Sask. R. 280, at para. 110. (see also *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, at paras. 119-24 and 134.) 위 항소심의 접근과는 대조적으로 판사 Caldwell는(Cameron도 동의함) 소송대상인 수색의 대상을 특징짓는 데 있어서 중요한 것은 “일상적인” 망이용계약자의 이름, 주소와 같은 신원정보의 이면의 것을 보는 것이라고 판단하였다. 신원정보로 라이프스타일의 세부사항과 개인의 선택이 노출될 수 있는 가능성은 당연히 고려되어야 한다고 판단하였다.: see also *Trapp*, per Cameron J.A., at paras. 33-37.

[26] 본 재판부는 이 쟁점에서 항소심 판사 Caldwell와 Cameron의 의견에 동의한다. 보통 수색의 대상을 정의하는 것은 논란의 여지가 없으나 이 사건의 경우 어려우므로 본 재판부는 경찰의 수사기법과 처분대상인 프라이버시 이익의 관계를 조사하는데 있어서 폭넓고 기능적인 접근을하기로 하였다. 본 재판부는 수색된 정보의 성격뿐만 아니라 수색된 정보가 노출시키는 정보의 성격도 고려하였다.

[27] 몇몇 판결이 이러한 접근방법을 택하고 있다. 정보프라이버시를 다루는 *Plant* 판결은 ‘자유민주사회의 구성원이라면 정부가 핵심적인 개인 신원정보를 전파하는 것을 통제하고 그 통제를 유지하고 싶어한다’며 정보에 관한 프라이버시를 강조했다. 또한 권리 헌장 제8장의 보호는 그 성격에 따른 정보를 보호하기위한 것만이 아니라 그 정보가 노출시키는 라이프스타일의 내밀한 부분과 개인의 선택까지 포함한다고 분명히 밝혔다.

[28] *Tessling*은 동일한 접근을 택하지만 다른 결론을 도출하여 수색의 본질을 ‘건물 표면에서 발생하는 열’로 본다. 적외선 전방 감시 장치 (Forward Looking Infra-Red 이하 FLIR) 기술은 주거 안에서 발생한 활동을 판단하는데 쓰이지만, 열 발생 자체로는 열발생원을 구별해낼 수 없다. 열 발생 자체로는 열을 발생시키는 정확한 활동을 추론할 수 없기 때문에 열

발생 자체는 무의미하다 : paras. 35-36. 중대한 문제는 매우 사적인 공간인 주거 내에서 발생한 활동을 추론하는데 FLIR 이미지가 뒷받침한 내용이다.

[29] 본 재판부는 *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456과 **companion appeal** in *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569를 검토하겠다. 법원은 다른 쟁점에서는 견해가 대립했으나 개가 Kang-Brown의 가방의 냄새를 맡은 것이 수색에 해당한다는 견해에는 만장일치로 긍정했다. 판사 Deschamps와 Bastarache가 설명했듯이 가방 부근의 냄새를 맡은 것은 가방 안에 있는 것에 대한 “강하고 신속하고 직접적인 추론”을 가능하게 한 수사절차로서 이루어졌다: Deschamps J., at paras. 174-75; Bastarache J., at para. 227. 그러므로 탐지견이 획득한 정보는 가방 부근의 공기의 냄새에 불과하지만 탐지견의 반응은 경찰이 가방 속의 물건에 대한 강한 추론을 이끌어냈다. 판사 Binnie는 A.M. 사건(피의자의 백팩을 개가 냄새맡도록 한 것에 대한 사건)에서 말했듯이 “탐지견을 사용함으로써 경찰은 가방의 천속을 들여다 ‘볼’ 수 있었다”고 판단했다. : para. 67.

[30] 소송대상인 수색 대상의 특징을 판단하는 방법은 최근에 *Gomboc*에서 다루었다. 다른 쟁점에서는 견해가 대립되었으나 수색의 대상을 결정하는데 적용될 틀에 대해서는 만장일치로 판단하였다. 법원은 디지털전류계기록장치(Digital Recording Ammeter: 이하 DRA)를 사용한 것이

수색에 해당되는지를 판단하기 위해 DRA의 데이터와 주거내에서 일어난 특정활동의 추론에 끼치는 영향을 고려하였다. 판사 Abella는 “주거 내의 특정 활동에 관해 전기 소비량의 패턴으로부터 만들어진 강하고 신뢰할 수 있는 추론”을 고려하였다(판사 Binnie, LeBel도 동의): para. 81. 대법원장과 판사 Fish는 DRA 데이터가 사적인 활동이 이루어지는 집안에 불을 키는 역할을 하는 것과 비유하였다: para. 119. 판사 Deschamps는 DRA 데이터가 주거내의 활동을 노출시키는 측면을 판단하였다: para. 38.

[31] 그러므로 수색 대상을 특징지을 때, 다른 개인정보와 관련하여 추론을 뒷받침하기 위해 반드시 획득한 정보의 경향성을 고려해야함은 분명하다. 판사 Doherty가 *Ward*에서 이에 적절한 접근방식을 설명하고 있는데, 소송대상인 수색의 대상을 정의하는데 있어서 법원은 “관련된 물리적인 행위와 침해된 물리적인 공간의 개념을 좁게 해석하지 말고, 정부의 행위로 인해 잠재적으로 손상된 프라이버시 이익의 성격을 참조 하여야 함”을 강조한다: *ibid.*

[32] 이 접근방식을 적용하여 본 재판부는 *Trapp*의 판사 Cameron의 의견을 반영한 판사 Caldwell의 의견에 동의한다. 수색의 대상은 단순히 Shaw와 계약을 맺은 사람의 이름과 주소가 아니라 특정 인터넷 활동과 대

응되는 인터넷 이용자의 신원정보(정체성)이다. *Trapp*의 판사 Cameron 의
견:

이런 종류의 정보의 성격을 단지 “망이용계약자의 정보”나 “고객 정보” 혹은 “이름, 주소, 전화번호”로 규정짓는 것은 이 정보의 성격을 불분명하게 만든다. 정보의 성격을 명확하게 규정짓지 않으면 IP주소의 중대성을 간과하기 쉬워 IP주소가 특정 개인으로 식별되어 그 개인의 주거내에서의 인터넷 활동을 포함한 개인정보의 노출까지 가능하게 된다.

[33] 수색의 대상은 자신의 인터넷 접속이 감시되는 특정 인터넷 활동과 연결된 망이용계약자의 신원정보이다.

(b) 국가의 행위에 의해 손상된 프라이버시 이익의 성격

[34] 국가의 행위에 관여된 프라이버시 이익의 성격은 상황의 총체성의 또다른 일면이며 프라이버시의 기대의 합리성을 판단하는데 중요한 요소이다. 대법원은 이전에도 정보 프라이버시를 비밀보호와 개인의 내밀한 정보의 통제의 개념으로 강조해왔다. 본 재판부는 온라인에서 프라이버시 이익을 보호할 때, 익명성의 역할을 설명하기 위해 이 사건의 처분대상인 프라이버시 이익을 다소 넓게 이해할 필요가 있다고 판단한다.

[35] 프라이버시는 “넓고 다소 덧없는 것”처럼 이해되고 있다: *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, at para. 67. 학자들은 프라이버시의 성격과 한계에 대한 이론적인 혼란과 사회적 합의의 부족함을 지적해왔다: e.g., C. D. L. Hunt, “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort” (2011), 37 *Queen’s L.J.* 167, at pp. 176-77. 이러한 문제점에도 불구하고 대법원은 프라이버시 이익을 장소적, 개인적, 정보적 등 세가지 종류로 구분했다. 서로 겹치는 부분도 있지만 프라이버시 이익의 성격이나 특정상황의 처분대상인 프라이버시 이익을 규정하는데 유용하다: e.g., *Dyment*, at pp. 428-29; *Tessling*, at paras. 21-24. 프라이버시 이익의 구분에 대한 설명은 엄격하거나 상호 배타적인 분류가 아니라 분석적인 도구이다.

[36] 프라이버시가 합법적이거나 불법적인 활동을 보호하는 것으로 프라이버시 이익의 성격을 결정짓지 않는다. 분석은 프라이버시 영역이나 수색 대상, 대상에 대한 수색의 영향에 달려있으며 수색물의 합법성이나 위법성에 의해 결정되지 않는다. *Patrick*에서 판사 Binnie의 의견을 다른 말로 바꾸어 표현하자면, 피고인이 아동 포르노에 접근한 것을 감추는 데 적법한 프라이버시이익의 존부는 쟁점에 해당하지 아니하지만, 일반적으로 자신의 주거에서 사적인 목적으로 컴퓨터를 사용한 것에 관하여 망이용계약자의 정보에 대한 프라이버시 이익이 인정되는지가 쟁점이다: *Patrick*, at para. 32.

[37] 본 재판부는 우선 정보프라이버시와 피고인이 피고인의 주거에서 감시당하였으므로 장소적 프라이버시 문제를 다루겠다. 그러나 활동이 일어난 장소는 부차적인 문제이다. 인터넷 이용자들은 집 밖에서 스마트폰이나 휴대용기기로 인터넷에 접속할 때에도 익명성의 기대를 가지고 인터넷 활동을 하기 때문이다. 그러므로 *Patrick*에도 언급됐듯이 주거는 통제요소가 아니지만 그럼에도 불구하고 상황의 총체성의 부분적인 요소에 해당한다: e.g., *Ward*, at para. 90.

[38] 정보프라이버시 문제로 다시 돌아가서, 프라이버시의 개념을 이해하기 위해서는 최소한 프라이버시를 서로 영역이 겹치더라도 3개의 개념으로 구분해야한다. 이는 비밀성, 통제성, 익명성이다.

[39] 정보프라이버시는 보통 비밀성과 동일시된다. 예를 들어, 환자는 담당의사가 그/그녀의 의료기록을 믿음과 신뢰로 보호할 것에 대한 합리적인 기대를 가지고 있다: see, e.g. *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, at p. 149.

[40] 프라이버시는 정보 이용과 접근에 대한 통제보다 더 넓은 개념을 포함하여 “개인, 단체, 기관이 정보가 어느 범위까지 언제, 어떻게 다른 사람에게 공유되는지 결정을 요구”하는 것을 의미한다: A. F. Westin, *Privacy and Freedom* (1970), at p. 7, cited in *Tessling*, at para. 23. 판사 La Forest는 *Dyment*에서 개인의 모든 정보는 개인이 소통하고 본인을 위해 향유하기 위해 적절한 방법으로 결정한다는 추정으로 얻어낸 통제로 정보 프라이버시를 이해하는 것을 강조했다(*Dyment*, at p. 429, quoting from *Privacy and Computers*, the Report of the Task Force established by the Department of Communications/Department of Justice (1972), at p. 13). 정보는 전달될 것이므로 비밀로 여겨질 수는 없지만, “그 정보의 수령자에게만 공개되고 그 공개된

목표로만 이용될 것이라는 합리적인 기대가 보호되어야 하는 상황들은 많다” (pp. 429-30); see also *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 46.

[41] 인터넷 이용의 맥락에서 특별히 중요한 정보프라이버시의 세 번째 개념은 바로 프라이버시를 익명성으로 이해하는 것이다. 본 재판부는 권리 헌장 제8장이 잠재적으로 보호하고 있는 프라이버시가 반드시 익명성의 개념도 포함해야한다고 판단한다.

[42] 설문에 응하는 사람은 고도로 사적인 정보가 될 수 있는 정보를 제공하기도 한다. 익명성도 프라이버시이다(*The notion of privacy as anonymity is not novel*). 익명성은 익명으로 이루어지는 설문조사부터 경찰 정보원의 신원보호까지 방대한 맥락에서 나타난다. 설문조사에 응하는 사람들은 매우 사적인 정보를 제공하는 것에도 선뜻 동의한다. 경찰 정보원도 범죄에 관한 정보를 제공한다. 정보 자체는 타인에게 전달되므로 사적인 것이 아니지만 정보는 제공하는 사람의 신원을 밝히지 않는다는 전제하에 전달된다. 경찰이 설문조사 결과와 대응되는 사람들의 이름 목록을 획득하고 싶어하거나 형사사건에서 피고인 측이 정보를 제공한 정보원의 신원을 알고 싶어하는 경우를 떠올려보자. 이러한 예에서 처분대상인 프라이버시이익은 단순히 개인의 이름이 아니라 신원이 밝혀진 개인과 익명으로 제공된 개인

정보이다. 캐나다인권협회의 제3자참가인은 익명성을 유지하는 것은 프라이버시를 보장하기 위한 필수적인 요소라고 진술했다: *factum*, at para. 7.

[43] Westin은 익명성을 프라이버시의 가장 기본상태로 규정한다. 익명성은 개인들이 신원확인과 감시로부터 자유롭게 공공장소에서 활동할 수 있게 한다: pp. 31-32; see A. Slane and L. M. Austin, “What’s In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations” (2011), 57 *Crim. L.Q.* 486, at p. 501. *R. v. Wise*, [1992] 1 S.C.R. 527에서의 대법원의 판단은 공공장소의 프라이버시의 예를 제시하며 공공도로(Public Highways)위의 차량소재를 언제 어디서나 감시하는 것은 용의자의 프라이버시의 합리적인 기대를 침해하는 것이라고 판단한다. 용의자가 공연하게 운전하는 것을 전자기기로 추적하는 것이 더 편리하다는 주장이 다뤄질 수 있었겠지만 대법원은 그러한 접근방식을 택하지 않았다.

[44] 판사 La Forest(s. 24(2)에 의해 증거를 배제하는 것에 반대의견, 프라이버시의 합리적인 기대 존재에 동의)는 “다양한 공적 맥락에서 우연히 관찰되는 것을 예상할 수 있지만, 집중적인 조사를 받는 것에 정당하게 격노할 수 있다. 이와 같은 공적 행위에서 우린 개인의 신원이 밝혀지고 대규모의 감시에 시달리는 것을 기대하지 않고, 상황적인 풍경속으로 알아

차릴 수 없게 녹아드는 것을 원한다”고 판단하였다: p. 558 (emphasis added), quoting M. Gutterman, “A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance” (1988), 39 *Syracuse L. Rev.* 647, at p. 706. 어떤 개인이 자신의 주거를 떠나서 공공장소에 들어간다는 사실만으로는, 그 개인이 공공장소에서 관찰당하는 것을 통제할 수 없음에도 불구하고, 그 개인이 그의 프라이버시권을 전부 포기한다고 말할 수 없다. 그러므로 맥락으로서의 프라이버시권을 보호하기 위해서 우리는 반드시 익명성을 프라이버시의 개념으로 인식해야한다: see E. Paton-Simpson, “Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places” (2000), 50 *U.T.L.J.* 305, at pp. 325-26; Westin, at p. 32; Gutterman, at p. 706.

[45] 인터넷 이용의 맥락에 있어서 정보프라이버시의 개념을 익명성으로 이해하는 것은 매우 중요하다. Westin이 설명했듯이 익명성의 한 형태는 사상을 공개적으로 알리고 싶어하지만 그 사상의 저자로 식별되는 것을 원치 않는 것이다: p. 32. 1970년에 출판된 Westin의 주장은 인터넷 커뮤니케이션의 한 종류의 특성을 수백만명이 접근 가능하지만 저자가 식별되지 않는 것으로 정확하게 예측하고 있다.

[46] 더욱이 인터넷은 저장된 인터넷 이용자의 정보의 양과 질을 기하급수적으로 증가시켰다. 사용기록을 훑어보는 것만으로도 이용자의 관심사에 대한 자세한 정보를 얻을 수 있다. 검색 엔진은 이용자의 검색기록을 수집할 것이고, 광고업자는 이용자의 웹사이트 방문기록을 추적하여 이용자의 관심사와 흥미를 개관할 수 있다. “쿠키(Cookies)”는 소비자의 습관과 웹사이트 내에서 선택된 옵션, 호스트 웹페이지 방문전후 방문한 웹페이지와 제공되는 개인정보를 추적하는데 쓰일 수 있다: see N. Gleicher, “Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web” (2009), 118 *Yale L.J.* 1945, at pp. 1948-49; R. W. Hubbard, P. DeFreitas and S. Magotiaux, “The Internet — Expectations of Privacy in a New Context” (2002), 45 *Crim. L.Q.* 170, at pp. 189-91. 이용자는 자신의 온라인 활동의 패턴을 감시당하는 것을 완전하게 통제할 수도 없고, 누가 관찰하는지도 알 수 없다. 하지만 정보와 개인사이의 연결고리를 보호하여 익명으로 인터넷을 이용한다면 꽤 많은 이용자가 자신의 인터넷 활동이 보호된다는 것을 확신할 수 있을 것이다: see Slane and Austin, at pp. 500-3.

[47] 본 재판부는 이용자의 인터넷활동과 연결된 개인의 신원정보는 정보에 내재된 이름, 주소, 전화번호 이상의 프라이버시법익을 발생하게 한다는 점에서 매우 중요하다고 본다. 마약 탐지견은 가방안의 내용물에 대한 정보를 제공하고 내용물과 관련된 프라이버시법익을 연관시킨다. **DRA**

측정값은 주거내의 활동에 대한 정보를 제공함으로써 활동과 관련된 프라이버시법익을 연관시킨다. 이와 유사하게 망이용계약자의 정보는 특정 종류의 정보를 식별가능한 개인과 연결시키면서 단순히 개인의 이름이나 주소가 아닌 정보의 근원, 소유자, 이용자로서의 신원과 관련된 프라이버시법익을 포함한다.

[48] 판사 Doherty는 *Ward*에서 자신만의 통찰력과 명료성으로 위 쟁점에 대한 논지를 명확히 밝혔다. 그는 개인적인 프라이버시는 개인이 개인의 성장과 열린 민주사회의 번영을 위해 필수적인 일정수준의 익명성을 유지하며 매일매일 사회의 구성원으로서 기능하는 능력을 보호한다고 판단한다: para. 71. 또한 일정수준의 익명성은 인터넷 활동의 특색으로 “상황의 총체성에 기해 익명성은 권리 헌장 제8장하에서 헌법적인 보호를 받을 수 있다”고도 결론을 내렸다: para. 75. 본 재판부는 이에 동의하여, 상황의 총체성에 기한 익명성은 부당한 압수와 수색에 반대하는 헌법적인 보호와 연관된 프라이버시법익의 근간이라고 주장하는 바이다.

[49] the Director of Public Prosecutions의 intervener은 익명으로 온라인 활동을 할 권리를 인지하는 것은 효율적인 수사 와 온라인 범죄기소를 방해해 범죄친화적 인터넷 환경을 구축할 것이라는 문제를 제기했다. 온라인으로 행해질 수 있는 범죄의 심각한 특성을 고려했을 때, 이 문제는 가볍게

여길 성질의 것이 아니다. 그러나 본 재판부는 상황에 따라 익명성의 프라이버시법익을 인정하는 것은 익명성의 어떤 권리든 인정하는 것에 못 미치며 인터넷에서 행해진 범죄와 관련된 수사의 효율성을 위협하지 않는다고 판단한다. 이 사건의 경우 경찰에게 Shaw로 하여금 IP주소와 대응되는 망이용계약자의 정보를 공개시키는 명령을 받을 충분한 정보가 있었던 것은 명백하다.

[50] 이 사건에 위의 사고들을 적용하는 것은 간단하다. 이 사건의 상황을 고려하면, IP주소와 망이용계약자의 정보를 연결시키는 수사 요청은 사실상 특정인(또는 공유한 인터넷 서비스를 이용하는 제한적인 수의 사람들)을 특정 온라인 활동과 연결시키는 것이다. 이런 종류의 요청은 익명으로 행해진 온라인 활동과 연결시키는 시도로 정보 프라이버시의 익명성 측면을 관련짓는데, 이 온라인 활동은 다른 상황에서 법원이 연관된 중대한 프라이버시법익으로 인정하였다: *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 3; *Cole*, at para. 47; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at paras. 40-45.

[51] 그러므로, 본 재판부는 경찰이 익명으로 이루어진 인터넷 활동을 특별히 감시하여 Shaw에게 망이용계약자의 정보를 요청한 것은 매우

높은 수준의 정보프라이버시에 부합한다고 판단한다. 하단의 Caldwell의 판단에 동의한다.

프라이버시 보호에 관심이 있는 합리적인 지식인이라면 자신의 주거에서 자신의 컴퓨터로 한 활동들이 사적으로 보호될 것이라고 기대할 것이다. 이 사건에서 개인적, 직접적으로 경찰의 활동에 노출된 것은 피고인이므로, 유출된 피고인의 여동생의 특성 정보와는 상관없다. 보통 말하는 경찰의 활동이 일단 보기에는 피고인의 개인적인 프라이버시권을 연루시키고, 이 점에 있어서 그의 유출된 정보의 프라이버시법익은 직접적이고 개인적이다 [para. 27]

(c) 프라이버시에 대한 합리적인 기대

[52] 다음 쟁점은 피고인의 프라이버시의 기대가 합리성 여부이다. 원심은 관련된 계약법적, 제정법적 조문에도 불구하고 프라이버시의 합리적인 기대가 없다고 판단하였다(판사 Caldwell도 항소심에서 이에 동의). (para. 19); para. 42. 판사 Cameron은 계약법적, 제정법적 조항이 이 사건의 맥락에서 영향을 끼쳤다고 판단하였다: para. 98.

[53] 본 재판부는 피고인이 계약법적, 제정법적 조항이 망이용계약자의 정보에 대한 프라이버시의 합리적인 기대를 약화시키지 않는다고 주장한다. 피고인은 계약법적 조항은 법에 의할 경우에만 경찰에게 정보가 제공된다는 것을 의미하고, 프라이버시권을 보호하는 개인정보보호및전자문서법은 이 사건의 프라이버시의 합리적인 기대의 존재를 지지한다고 진술하였다. 검사는 피고인의 의견에 동의하지 않고 항소심의 판사 Caldwell의 의견에 동의하였다.

[54] 계약 및 제정법의 체계가 관련성은 있지만 프라이버시의 합리적인 기대의 존부 판단에 필요한 결정요인이 아니라는 것에는 이견이 없다. *Gomboc*에서 판사 Deschamps는 네명의 재판관을 대표하여 전기공급자와 고객간의 관계를 규율하는 용어는 피고인의 프라이버시의 합리적인 기대에 “대단히 중대”하지만 “상황의 총체성을 판단하는 다수의 요소 중 하나”로 다루었다: paras. 31-32. 또한 소비자 관계의 맥락에서 부합계약을 다룰 때, 특정 조문이 프라이버시의 합리적인 기대에 영향을 끼칠 경우 “조심스럽게 진행”하는 것의 중요성을 강조하였다: para. 33. 이 맥락에서 주의의 필요는 주심과 판사 Fish가 반대의견에서 날카롭게 강조하였다: paras. 138-42.

[55] 이 사건에서 Shaw의 이용약관은 개인정보보호및전자문서법을 참조하였으므로 계약 및 제정법의 체계가 서로 겹치고, 이때 개인정보보호 및전자문서법상 허용된 정보 공개범위는 고객이 개인정보의 공개에 동의했는지 여부에 달려있다. 우선 이 체계의 세부사항들을 소개한 후에 이것이 합리적인 기대에 대한 분석에 미치는 영향을 검토할 것이다. 관련된 조항이 피고인의 프라이버시의 기대의 합리성을 판단하는데 약간의 도움을 줄 뿐이라는 것은 명확해진다.

[56] Shaw는 고객에게 서비스 약관에 기해 인터넷 서비스를 제공하는 회사이다. 추가되는 항목과 조건은 "망이용목적 제한 방침"와 "개인정보보호방침"에 제공된다. 약관의 항목들은 Shaw의 웹사이트에 게재되고 종종 변경된다. 수사관은 2007년 8월 31일에 쓰인 IP주소에 대한 망이용계약자의 정보를 Shaw에 요청하였다.

[57] 피고인은 피고인의 여동생의 명의로 인터넷에 접속했으므로 이 사건 이용약관의 당사자가 아니다. 관례상 여러 이용자가 하나의 인터넷 명의를 공유하는 것은 흔한 일이다. 합리적인 이용자라면 서비스를 이용할 때 특정 항목과 조건이 적용되며 관련 사항들이 인터넷에 게재되어 있어 손쉽게 접근할 수 있다는 걸 인지하고 있을 것이다. 이 사건은 피고인에게

Shaw와의 계약내용이 적용되는지 여부를 판단할 필요가 없다. 계약상 책임과는 다르게 피고인이 인터넷에 접속한 것은 피고인의 프라이버시에 대한 합리적인 기대를 판단하는데 적절한 상황이다. 본 재판부는 이 사건에서 피고인에게 Shaw의 이용약관이 적용되는지 판단할 필요가 없다고 본다. 계약상 책임과는 별도로 피고인이 인터넷에 접속하면서 얻은 권리는 피고인의 프라이버시의 기대의 합리성을 판단하는 것과 관련된 요소이다. 망이용 계약자의 정보를 요구하는 경찰의 요청에 Shaw가 취할 행동에 대해, 관련된 세 그룹의 조항은 모호하고 불확실한 관점을 제시한다. “Shaw는 합법적, 단속적이거나 다른 정부 기관의 요청에 의해 필요할 경우 어느 정보든 공개할 수 있다”는 조항은 언뜻 보기에 “이용약관”이 넓은 범위의 정보 공개를 허용하는 것처럼 보인다. 그러나 이 일반 규정은 IP 주소와 범죄수사 프라이버시 정책의 대상이 되는 “망이용목적 제한 방침”에 포함된 범죄수사의 맥락에서 식별된 정보나 IP주소를 공개하는 특별규정으로 보아야 한다.

[58] 망이용목적 제한 방침(2007년 6월 18일에 가장 최근 변경됨)은 Shaw가 개인정보보호방침에 따라서 망이용계약자의 신원을 식별할 수 있는 정보를 제공하는 것을 포함한, 범죄수사를 위해 경찰과 협조할 수 있으며 이에 따라 이용자 신원정보를 제공할 수 있다는 내용을 포함하고 있다. 관련 조항은 다음과 같다.

귀하는 이로써 Shaw가 (i) 범죄수사를 위해 경찰과 협조할 수 있고 (ii) 다른 망사업자, 네트워크, 전산 설비시스템의 관리자가 이 이용약관을 시행하는 것에 협조하는 것을 동의합니다. 이에 Shaw의 개인정보보호방침에 따라서 사용자 명, IP 주소 등 이용자를 식별할 수 있는 다른 정보를 포함할 수 있습니다.

[59] 기록의 개인정보보호방침(2008년 11월 12일에 가장 최근 변경됨)은 Shaw가 식별가능한 개인에 관한 정보로 정의되어 있는 개인정보를 보호하는 것에 전념하고 있다고 밝히고 있다. 이 지침에 명시된 열가지의 원칙중 하나는 개인정보 공개의 제한에 관한 원칙이다(원칙 5). 이 원칙은 “법으로 허용된 예외적인 상황”에 대한 고객의 동의나 인지 없이 개인정보가 공개되는 상황을 제한하고 있다. Shaw는 서비스를 제공하기 위해 사업 파트너에게 정보를 제공할 수 있으며 그 정보는 개인정보보호및전자문서법에 따르고, 엄격한 비밀 유지 기준과 정책에 의해 규율되어야 한다. 또한 이 방침은 법에 의해 강제되는 경우나 고객이 동의를 한 경우에만 개인정보보호및전자문서법에 따라서 Shaw가 고객의 개인정보를 제3자에게 제공할 수 있다고 명시하고 있다.

[60] Shaw가 개인정보를 공개한 것이 법에 의해 허용되거나 의무인 것과 상관없이, 이는 적용가능한 제정법적 체계의 분석에 따라 달려있다.

계약상 조항을 전체적으로 살펴볼 경우 망이용계약자의 정보를 요청한 경찰과의 관계에 있어 이용자의 프라이버시의 합리적인 기대에 끼치는 영향이 모호하고 불확실함을 알 수 있다. 개인정보보호및전자문서법상의 제정법의 체계도 이에 큰 도움이 되지 않는다.

[61] Shaw가 수집, 이용, 공개하는 망이용계약자의 개인정보는 상업적인 활동에 관여하는 기관이 지닌 개인정보가 정보와 관련된 사람의 동의나 인지 없이 공개되는 것으로부터 보호하는 개인정보보호및전자문서법의 대상이다: Sch. 1, clause 4.3. 제 7장은 일반 원칙의 예외를 규정하고 있으며 기관이 동의 없이 개인정보를 공개하는 것을 허용하고 있다. 이 사건에서 적용된 예외는 s. 7(3)(c.1)(ii)이다. 이 조문은 수사를 위해 정보공개 요청을 한 정부기관과 정보요청에 합법적인 권한이 있는 경우 정보공개를 허락하는 내용을 담고 있다. 개인정보보호및전자문서법의 규정들은 이 사건에서 프라이버시의 합리적인 기대 존부를 판단하는데 큰 영향을 끼치지 않는다. 순환논리로 이끌 뿐이다.

[62] 7(3)(c.1)(ii)는 동의 없이 정부기관이 정보를 획득하는데 합법적인 권한이 있다고 판단할 경우 정보 공개를 허용하고 있다. 그러나 결과적으로 합법적인 권한의 존부 여부는 망이용계약자의 정보에 대하여 프라이버시의 합리적인 기대가 있었는지에 달려있다. 그러므로 관련된 조항을

해석할 경우 조항 자체가 프라이버시의 합리적인 기대 존부에 기대고 있으므로, 개인정보보호및전자문서법은 프라이버시의 합리적인 기대의 존부를 판단하는 기준이 될 수 없다. 개인정보보호및전자문서법의 목적은 개인정보를 공개하는 것이 어떤 의미로는 자신의 개인정보에 대하여 개인의 프라이버시권을 인정하는 것을 규율하는 것이므로(s. 3), 경찰의 단순한 요청으로 개인정보를 공개할 의무가 발생한다거나, 동의 없이 개인정보를 공개하는 것을 일반적으로 금지하는 개인정보보호및전자문서법에 반하는 행위가 일어나지 않으리라고 인터넷 이용자가 기대하는 것이 합리적이라고 할 수 있다.

[63] 본 재판부는 망이용계약자의 프라이버시의 합리적인 기대를 판단하는데 개인정보보호및전자문서법의 규정이 요소로 고려된 *Ward*의 Ontario 항소심과는 다른 결론을 도출하였다. 이러한 결론은 중요한 두가지 쟁점을 고려하여 도출된 것인데, 첫 번째 쟁점은 ISP의 서비스를 이용하여 저질러진 범죄의 수사에 협조하는 것에 타당한 이익이 있다는 것이다: para. 99. 두 번째 쟁점은 ISP가 경찰의 수사에 협조하는 것이 아동 포르노의 심각성을 고려하면 합리적이라는 점이다: paras. 102-3. 이러한 고려가 정책적인 입장에서는 당연히 연관되어 있지만, 정보 공개 요청이 합법적인 권한이 있는 정부기관에 의해서만 이루어진 경우 정보공개를 허용하는 개인정보보호및전자문서법의 s. 7(3)(c.1)(ii)에 명백한 제정법적 명문의 의미를

무시할 수는 없다. 개인정보보호및전자문서법의 제한을 받고 있는 기관이 개인정보에 관한 법률상 의무를 지킬 것이라고 기대하는 것은 타당하다. *Ward*의 항소심은 s. 7(3)(c.1)(ii)는 “상황에 적합하게 합리적인 개인이 고려할 경우에만 단체가 개인정보를 수집, 이용, 공개할 수 있음을 명시하는 s. 5(3)을 감안하여 적용되어야 한다”고 판단했다. “합리적인 공개”의 원칙은 ISP가 경찰에 협조하고 개인정보보호및전자문서법의 해석에 따른 심각한 범죄를 예방하는 것에 대한 고려를 환기시키는 근거로 사용되었다. 제5장 (3)은 개인정보보호및전자문서법의 다양한 규정의 해석을 뒷받침하는 원칙이다. 이 원칙은 명확한 필요요건인 “적법한 권한”이 결여된 정부기관의 요청을 허용하지 않으며, 프라이버시의 합리적인 기대 존부를 판단하는 요소로 s. 7(3)(c.1)(ii)를 사용하는 것의 본질적인 순환성을 해결하지 못한다.

[64] 나는 ISP가 자신의 서비스를 통해 발생하는 범죄를 예방하고자 하는 정당한 이익을 인정하며 ISP 스스로 불법행위를 포착하고 자발적으로 경찰에 통보하는 경우에는 완전히 다른 고려사항들이 적용된다고 본다. 이러한 상황은 개인정보보호및전자문서법 s. 7(3)(d)의 넓은 면제사유에 각각 해당하게 된다. 이 사건 수사의 경우 경찰의 수사로 시작되었으며 망이용계약자의 정보 유출은 경찰이 *Shaw*에게 요청한 것으로부터 발생했다.

[65] 전체적으로 살펴본 이 조항은 법으로 강제되거나 허용될 경우에만 경찰의 요청에 응해 정보를 공개하게 되어 있다. 이는 개인정보보호및 전자문서법 s. 7에 의해서만 허용되며 이 사건의 경우 정보 공개를 요청하기 위해 경찰은 “적법한 권한”이 있어야 한다. 다음에 설명할 이유로 인해 이 요청은 적법한 권한이 없으며 경찰은 요청을 준수하게 할 권한이 없다. 프라이버시 방침이 Shaw가 망이용계약자의 개인정보를 공개할 권리를 좁게 제한하고 있으므로 본 재판부는 이 사건의 어느 계약상 조항이 프라이버시의 합리적인 기대의 존재를 뒷받침하는 것으로 판단한다.

[66] 본 재판부는 이 사건의 상황의 총체성을 토대로 망이용계약자의 정보에 프라이버시의 합리적인 기대가 있다고 판단한다. 이러한 정보의 공개는 익명성을 기대하고 이루어지는 내밀하거나 민감한 온라인 활동을 하는 이용자의 신원을 식별할 수 있게 할 것이다. 경찰의 요청으로 ISP가 자발적으로 공개한 정보는 수색에 이르게 된다.

[67] Alberta 법무장관은 경찰이 망이용계약자의 정보 공개를 요청하는 것이 허용되지 않는다면, 피의자의 민감정보가 노출될 수 있는 다른 통상적인 수사 또한 금지될 것이고 이는 과도하게 범죄수사를 방해하는 것이라는 문제점을 제기했다. 예를 들어, 경찰이 범죄 피해자를 면담할 경우 피

의자의 라이프스타일에 대한 핵심적이고 자세한 정보가 노출될 수 있다는 것이다. 본 재판부는 이러한 원칙에 따른다고 해서 반드시 위의 결과가 발생할 것이라는 주장에 동의하지 않는다. 경찰이 제3자에게 피의자와 관련된 정보를 요청하는 것이 수색에 해당되는지는 상황의 총체성에 기해 피의자가 그 정보에 관해 프라이버시의 합리적인 기대를 가지고 있는지에 달려 있기 때문이다: *Plant*, at p. 293; *Gomboc*, at paras. 27-30, *per Deschamps J. Duarte* 에서 대법원은 개인이 경찰에게 피의자와의 대화를 전하는 것과 이 대화를 녹음한 파일을 입수한 것을 구별하였다. 또한 대법원은 위험은 “대화를 진술하는 것이 아니라 정부로 하여금 대화를 녹음하고 전송하는 것에 제한없는 재량권을 부여하는 것의 내재적인 위험”을 의미한다고 명시했다: at pp. 43-44. 이 사건에서도 유사하게 경찰은 ISP에게 이용자의 정보를 요청했으며, 이는 사실상 특정 온라인 활동을 감시하던 경찰을 피고인과 연결시킴으로 인해 단순한 질문과 같은 수사의 과정보다 더 중요한 프라이버시법익을 관여시켰다.

B. 수색은 합법적이었는지

[68] 이 사건과 같은 무영장수색은 부당한 것으로 추정된다: *R. v. Collins*, [1987] 1 S.C.R. 265. 검사는 이 추정을 반증할 책임을 진다. 수색은 (a) 법에 의해 허용된 경우 (b) 법 자체가 타당한 경우 (c) 수색이 타당한

절차에 의해 이루어졌을 경우, 타당한 수색에 해당하게 된다: p. 278. 피고인은 수색을 허락할 것을 의도했다고 볼 수 있는 법의 위헌성을 다투지 않았다. 대신 수색의 절차적 타당성에 이의를 제기했는데, 본 재판부는 이유 없다고 판단한다. 그에 맞춰 본 재판부는 수색이 법에 의해 허용되었는지만 판단한다.

[69] 검사는 항소심의 판사 Caldwell과 Cameron의 견해를 지지하여 형법 s. 487.014과 개인정보보호및전자문서법 s. 7(3)(c.1)(ii)가 적용된 수색은 합법적이라고 주장하였지만 본 재판부는 이에 동의하지 않는다.

[70] 형법 Section 487.014(1)는 보안관이 “법으로 공개가 금지되지 않은 문서, 데이터, 정보를 자발적으로 제공할 것을 요청”하는 데 수행명령이 필요하지 않다고 규정하고 있다. 개인정보보호및전자문서법은 정부기관이 획득(단순히 정보를 요청하는 것과 다름)하는데 필요한 적법한 권한을 드러내는 경우를 포함하여, 수사요청의 필요요건이 충족되지 않는 한 정보공개를 금지하고 있다: s. 7(3)(c.1)(ii). 검사가 해석한 이 조항 상 경찰의 개인 정보 요청에도 불구하고 개인정보보호및전자문서법의 보호는 사실상 무의미해진다: 단순 요청이 있으므로 기관이 정보를 공개하는 것은 더 이상 법으로 금지되는 것이 아니므로 “적법한 권한”은 권한 없이 강제하는 것이 된다.

[71] 개인정보보호및전자문서법 7(3)(c.1)(ii)의 “합법적인 권한”은 동의 없이 개인정보를 제공할 수 있는 경우에 해당하는 “법원이나 사법권이 있는 사람, 기관에 의한 소환장, 영장, 명령에 준수하여 정보나 기록을 제공해야한다”고 규정하고 있는 7(3)(c)와 분명히 구별되어야한다. s. 7(3)(c.1)(ii)의 “적법한 권한”은 “소환장 혹은 [수색]영장” 이상의 것을 의미한다. “적법한 권한”은 다양한 것을 포함할 수 있다. 경찰이 프라이버시의 합리적인 기대가 없는 대상에 대하여 질문을 할 수 있는 관습법상의 적법한 권한을 참조할 수 있다. 또한 긴급한 상황이나 타당한 법에 의해 허용된 경우 영장없이 행해진 수색을 한 경찰의 권한을 참조할 수 있다: *Collins*. the Privacy Commissioner of Canada의 intervener은 s. 7(3)의 맥락에서 “적법한 권한”은 가장 기본적인 것만 갖춘 수사요청보다 더 엄격함을 요구한다는 점에서 중요한 역할을 하며 다른 대체적인 의미보다 더 우선되어야 한다고 진술했다. 요약하면, 본 재판부는 형법 487.014(1)나 개인정보보호및전자문서법이 경찰이 압수, 수색할 수 있는 권한을 발생시키지 않는다는 점에서 *Ward* 의 Ontario 항소심의 판단에 동의한다: para. 46.

[72] 본 재판부의 결론은 *Trapp*에서 Saskatchewan 항소심이 내린 결론과 *R. v. McNeice*에서 British Columbia 대법원이 내린 결론과 2010 BCSC 1544 (CanLII)의 대법원이 내린 결론과 다르다. *Trapp*의 항소심은 s. 487.014(1)과 개인정보보호및전자문서법 7(3)(c.1)(ii)과 유사한 정보의자유와

프라이버시보호법(*Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01) s. 29(2)(g)를 “적법한 권한” 요건이 결여 되어있음에도 개인정보보호및전자문서법 s. 7(3)(c.1)(ii)과 유사한 조항으로 해석한다. 법원은 s. 487.014(1)이 경찰이 어느 수사(법으로 금지되지 않았다면)든 수행할 수 있는 권한을 발생시키는 것으로 보았다. *McNeice*의 재판부는 이 사건 조항에 해당하는 개인정보보호및전자문서법 s. 7(3)(c.1)(ii)와 관련된 사건에서 동일한 접근방식을 택하였다.

[73] 대단히 죄송하지만 본 재판부는 이 결론을 개인정보보호및전자문서법 7(3)(c.1)(ii)에 적용하는 것을 허용할 수 없다. 487.014(1)가 “**확실히 해두자면**”으로 시작함을 고려하여 이 조항은 경찰의 수사를 승인하는 현존하는 관습법상의 권한을 확인하는 선언적인 규정에 해당한다: see *Ward*, at para. 49. 개인정보보호및전자문서법의 입법 목적은 s. 3에 명시되어 있듯이 개인정보를 더 강하게 보호하기 위함이다. 이 사건 상황에서 긴급한 상황과 타당한 법의 결여로 경찰은 망이용계약자의 정보에 대한 수색을 수행할 권한이 없으므로, 본 재판부는 선언적인 규정과 개인정보를 더 강하게 보호하기 위한 규정의 조합으로 새로운 수색권한을 얻을 수 없다고 판단한다.

[74] 경찰이 획득한 망이용계약자의 정보없이 영장이 발급되지 않았을 것이므로, 이는 피고인의 여동생의 주거를 수색할 영장을 발급받는데 근거가 되었다. 불법적으로 획득된 그 정보를 판단에서 배제시켰다면 영장을 발급받을 타당한 근거가 결여되었을 것이고 이는 결국 주거를 수색한 것이 불법인 것으로 귀결된다. 그러므로 본 재판부는 피고인 여동생의 주거를 수색한 행위는 권리헌장을 위반한 것으로 판단한다: *Plant*, at p. 296; *Hunter v. Southam*, at p. 161. 그 어느 이유도 경찰이 임박한 신체적 위해를 예방하기 위해 정보가 필요한 경우 등의 긴급상황에 정보를 획득할 수 있는 경찰의 권한을 약화하거나 다루지 않는다.

C. 증거가 배제되어야 하는지

[75] 원심 재판부와 항소심은 이 사건에서 권리헌장 제8장 위반이 일어나지 않았다고 판단하였으므로 피고인의 권리헌장의 권리를 위반한 사유로 권리헌장 s. 24(2)에 의해서 획득된 정보를 증거에서 배제시켜야 하는지 판단할 필요가 없었다. 증거사용을 허용하는 것이 사법부의 신뢰를 떨어뜨렸는지 여부가 주요 쟁점이다. 피고인과 검사가 동의하듯이 이 쟁점을 공식적으로 결정할 수 있지만, 본 재판부는 피고인의 증거가 배제되어야 한다는 주장에 대해서 동의하지 않고 증거로 사용되어야 한다고 판단한다.

[76] s. 24(2)를 적용하는 방법은 *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353에 명시되어 있다. 재판부는 “증거를 채택하는 것이 사법부에 대한 사회의 신용에 끼치는 영향을 다음의 요소를 고려하여 판단해야 한다. (1) 권리 헌장을 침해하는 국가의 행위의 심각성 (2) 피고인의 권리헌장상 보호받을 법익의 침해효과 (3) 판결에 대한 사회적인 관심.”: para. 71.

[77] 국가 행위의 심각성을 우선 검토하자면, 본 재판부는 “권리헌장을 의도적 혹은 명백하게 묵과한 것”이라고 볼 수 없다고 판단한다: *Grant*, at para. 75. 수사관 Parisien은 Shaw에게 요청한 것이 법에 의해 허용된 것이라고 신뢰했으며 Shaw가 정보를 제공하는 것에 동의했다고 보았다. 그는 그러나 이것이 법적으로 타당한 관행인가에 대해서는 결정이 나뉜다는 것을 알고 있다고도 증언하였다. 본 재판부는 판단하기 애매모호한 영역에서 경찰이 영장없이 행동하는 것을 독려하는 것은 아니지만, 원심 재판부와 항소심의 세 명의 재판관이 수사관 Parisien이 적법하게 행동했다고 판단하였고, 그의 행위가 법으로 허용된 것이라고 믿은 것은 타당한 것으로 보인다. 요약하면 경찰은 중요한 수사를 할 목적으로 자신이 적법하다고 신뢰한 방법으로 행동하였으므로, 어느 측면으로도 수색영장을 획득하게 한 정보에 대하여 이견이 없다. 이 사건에서 경찰의 행위의 성격은 사법부의 평판을 떨어뜨리지 않는다.

[78] 두 번째 주요 요소는 피고인의 권리헌장상의 보호법익을 침해하는 행위가 끼치는 영향이다. 이 사건에서 그 영향은 심각하다. 위에 논의한 바와 같이 익명성은 온라인상의 프라이버시법익에서 중요한 안전장치이다. 익명성의 침해는 피고인의 개인적인 선택을 노출시키며 피고인을 경찰의 수사의 대상으로 만들었다. 이는 증거를 배제하는 의견을 뒷받침 한다.

[79] 마지막 요소인 본안판결에 대한 사회의 관심은 다음과 같이 *Grant*에서 설명하고 있다.

기소된 범죄의 종류가 심각하여 본안결정에 대한 사회의 관심이 고조되어 있으며, 특히 피의자에 대한 **penal stake**가 높은 경우 사회는 사법시스템이 비난을 받지 않는 것에 필수적인 관심을 갖고 있다 [para. 84]

[80] 이 사건에서 피고인이 기소된 범죄는 그 성질이 중한 것이고 최소 징역형에 해당한다. 사회는 이 사건의 판결과 이러한 심각한 종류의 범죄를 취급하는 사법 시스템이 비난의 여지가 없는 것에 대한 강한 관심이 있다. 증거가 배제된다면 검사는 실질적으로 기소를 유지할 수 없을 것이다. 이의가 제기되는 증거(아동포르노를 포함한 전자파일)는 신뢰성이 있으며 공판정에서 변론에 의해서도 아동포르노로 여겨졌다. 사회는 의심할 여

지가 없이 신뢰할만한 증거에 기한 공정한 재판을 기대하며 아동의 안전과 관련된 범죄에 관한 재판일 경우 더더욱 그러하다.

[81] 위의 세요소를 고려하여, 본 재판부는 증거를 허용하지 않고 배제하는 것이 오히려 사법부에 대한 신뢰를 떨어뜨릴 것이므로 증거로 사용하는 것을 인용한다.

D. 제공행위에 대한 기소의 흠결요소

[82] 항소심은 원심이 제공행위에 대한 판단에 법리적인 오해가 있으므로 이에 대해 재심을 명령했다. 항소심은 원심이 제공행위 혐의가 성립되기 위해서, 피고인이 자신의 적극적인 행위가 다른 이들의 포르노 접근을 촉진시켰다는 것에 대해 선의여야 한다고 판단한 부분에서 법리적 오해가 있다고 보았다. 이 오해로 원심은 포르노가 공유폴더에 의해서 다른 사람들에게 제공된 것에 피고인이 의도적인 백안시였는지 판단하지 못했다. 본 재판부는 두가지 측면에서 항소심의 판단을 지지하며 재심을 명령한 것을 인용한다.

[83] s. 163.1(3)에 의해 기소된 피의자가 포르노 자료가 제공되고 있다는 것을 알고 있다는 것에 대해 입증되어야 함에는 이견이 없다. 그러나 원심이 제안하듯이 피의자가 적극적인 행위를 통해 고의로 자료의 제공성을 촉진할 필요는 없다. 본 재판부는 다음의 판사 Caldwell의 견해를 지지하여 피의자가 고의로 포르노를 타인에게 제공한 것으로 혐의가 성립한 것으로 판단한다.

s. 163.1(3)상의 아동포르노 제공행위의 고의 성립요건은, 프로그램을 통하거나 파일 공유 프로그램이 타인에게 파일을 제공한다는 지식이 있는 상황에서 아동 포르노를 포함한 컴퓨터 파일을 타인에게 제공했다는 고의를 입증하는 증거가 필요하다.[para. 87]

이 지점에서 원심의 판단 이유가 다양하게 해석될 수 있지만, 전체적으로 해석할 경우 본 재판부는 제공행위의 고의 성립요건을 만족시키기 위해서 적극적인 행위가 필요하다는 부분에서 원심이 법리를 오해했다고 주장한 판사 Caldwell의 견해를 지지한다: para. 81.

[84] 더 나아가 본 재판부는 판사 Caldwell의 의견에 동의하여, 의도적 백안시를 추론하는 것을 지지하는 증거에 전념하지 않아 원심이 적극적인 촉진에 관해 오해하였으므로 증거에 관해 의도적 백안시가 당면 문제인

것을 인정한다. *R. v. Briscoe*, 2010 SCC 13, [2010] 1 S.C.R. 411, at para. 21에서 판사 Charron가 설명하듯이 미필적 고의는 고의를 대체할 수 있다.

미필적 고의는 특정 혐의에 대한 범의를 규정하지 않고, 오히려 고의가 범의의 구성요소일 경우 고의를 대체할 수 있다. 미필적 고의는 피의자가 의심을 갖게 되어 추가적인 탐구를 해야할 필요를 느끼지만 의도적으로 그런 탐구를 하지 않을 때 피의자가 인지를 한 것으로 간주한다. See *Sansregret v. The Queen*, [1985] 1 S.C.R. 570, and *R. v. Jorgensen*, [1995] 4 S.C.R. 55. 판사 Sopinka가 *Jorgensen* (at para. 103)에서 간결하게 표현했듯이 “미필적 고의를 밝히는 것은 다음 질문에 대해 긍정적인 답을 하는 것을 포함한다. 피의자가 보는 것으로 피의자가 고의가 될 것을 강하게 의심하여 눈을 감았는가 혹은 고의로 눈을 감았는가?”

[85] 미필적 고의를 고려할 때 피고인이 경찰에게 진술한 다음 내용과 같은 증거를 필요로 한다. 피고인은 이 사건 프로그램이 파일공유 프로그램임을 알고 있었음, 피고인은 이 사건 프로그램이 처음 설치되었을 때 최소 하나의 설정값을 변경하였음, 이 사건 프로그램은 사용될 때마다 이 용자에게 이 프로그램이 파일 공유 프로그램임을 공지함, 이 사건 프로그램은 파일 공유로 인한 영향을 경고함, 이 사건 프로그램은 다른 이용자의 컴퓨터에 다운로드 되고 있는 상황을 보여주는 시각적인 지표를 갖고 있음: paras. 88-89.

[86] 미필적 고의가 당면 문제인 것과 제공행위에 대한 혐의의 주관적인 구성요건이 성립하기 위해 적극적인 행위가 필요하다는 원심의 판단이 결과적으로 미필적 고의를 고려하지 않게 하였으므로, 본 재판부는 판사 Caldwell의 의견에 동의하여 이 오해가 무죄판결을 내린 것에 영향을 준 것으로 판단될 수 있다고 본다: para. 93; *R. v. Graveline*, 2006 SCC 16, [2006] 1 S.C.R. 609, at para. 14.

III. 이유

[87] 본 재판부는 상고를 기각하고 소지 혐의에 대한 유죄를 인정, 제공행위 혐의에 대한 항소심의 판단을 인용하여 재심을 명령한다.

[1]

[1]

[2]

[3]

I. 부속

[4] 개인정보보호및전자문서법(*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5)

7. ...

(3) [인식이나 동의없는 공개] clause 4.3 of Schedule 1 의 목적을 위해서 그리고 그 조항의 부속각주에도 불구하고, 단체는 개인정보를 그 개인의 동의나 인지 없이 다음과 같은 상황에서 공개할 수 있다

...

(c) 정보제출을 강제할 수 있는 법적 권한이 있는 법원, 사람 또는 기구가 발부한 소환장, 영장 또는 명령을 준수하기 위해 필요한 경우, 또는 기록제출에 대한 법원의 규칙을 준수하기 위해 필요한 경우

(c.1) 공개가 해당 정보를 요청하고 그 정보를 취득할 법적 권한을 제시한 정부기관이나 그 일부에게만 이루어지며

...

(ii) 공개가 캐나다, 주정부 또는 해외관할의 법을 집행함에 있어 요구되거나, 그런 법집행과 관련된 수사나 정보수집을 수행함에 있어 요구되는 경우

...

(d) 정부기관 또는 그 일부 또는 수사기관에게 기구의 주도로 이루어졌고

(i) 그 기구가 해당정보가 캐나다 법, 주법 또는 외국법의 위반 또는 계약위반이 범해질 것을 알기에 합리적인 근거를 가지고 있거나 , 또는

(ii) 그 기구가 해당정보가 국가안보, 캐나다 국방 또는 국제업무에 유관하다고 의심하는 경우;

[5] ...

[6] 캐나다형법 [생략]

Appeal dismissed.

Solicitors for the appellant: McDougall Gauley, Regina.

*Solicitor for the respondent: Attorney General for Saskatchewan,
Regina.*

*Solicitor for the intervener the Director of Public Prosecutions: Public
Prosecution Service of Canada, Edmonton and Halifax.*

*Solicitor for the intervener the Attorney General of Ontario: Attorney
General of Ontario, Toronto.*

Solicitor for the intervener the Attorney General of Alberta: Attorney General of Alberta, Calgary.

Solicitors for the intervener the Privacy Commissioner of Canada: Osler, Hoskin & Harcourt, Toronto.

Solicitors for the intervener the Canadian Civil Liberties Association: Kapoor Barristers, Toronto.

Solicitors for the intervener the Criminal Lawyers' Association of Ontario: Dawe & Dineen, Toronto; Schreck Presser, Toronto.