novática
Revista de la Asociación de Técnicos de Informática

Novática, founded in 1975, is the oldest periodical publication amongst those specialized in Information and Communications Technology (ICT) existing today in Spain. It is published by **ATI** (*Asociación de Técnicos de Informática*) which also publishes **REICIS** (*Revista Española de Innovación, Calidad e Ingeniería del Software*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI is a founding member of **CEPIS** (Council of European Professional Informatics Socities), an organization with a global membership of above 200,000 European informatics professionals, and the Spain's representative in **IFIP** (International Federation for Information Processing), a worldwide umbrella organization for national societies working in the field of information processing. It has a collaboration agreement with **ACM** (Association for Computing Machinery) as well as with **AdaSpain**, **AI2**, **ASTIC**, **RITSI** and **Hispalux** among other organisations in the ICT field.

Editorial Board
Ignacio Agulló Sousa, Guillem Alsina González, María José Escalona Cuaresma, Rafael Fernández Calvo (Chairman), Jaime Fernández Martínez, Luis Fernández Sanz, Didac Lopez Viñas, Celestino Martín Alonso, José Onofre Montesa Andrés, Francesc Noguera Puig, Ignacio Pérez Martínez, Andrés Pérez Payeras, Viktu Pons i Colomer, Juan Carlos Vigo López

Chief Editor
Llorenç Pagés Casas <pages@ati.es>
Layout
Jorge Llácer Gil de Ramales
Translations
Grupo de Lengua e Informática de ATI <http://www.ati.es/gt/lengua-informatica/>
Administration
Tomás Brunete, María José Fernández, Enric Camarero

Section Editors
Artificial Intelligence
Vicente Botti Navarro, Vicente Julián Inglada (DSIC-UPV), <{vbotti,vinglada}@dsic.upv.es>
Computational Linguistics
Xavier Gómez Guinovart (Univ. de Vigo), <xgg@uvigo.es>
Manuel Palomar (Univ. de Alicante), <mpalomar@dlsi.ua.es>
Computer Archiecture
Enrique F. Torres Moreno (Universidad de Zaragoza), <enrique.torres@unizar.es>
José Flich Cardo (Universidad Politénica de Valencia), <jflich@di9sca.upv.es>
Computer Graphics
Miguel Chover Sellés (Universitat Jaume I de Castellón), <chover@lsi.uji.es>
Roberto Vivó Hernando (Eurographics, sección española), <rvivo@dsic.upv.es>
Computer Languages
Óscar Belmonte Fernández (Univ. Jaime I de Castellón), <belfern@lsi.uji.es>
Inmaculada Coma Tatay (Univ. de Valencia), <Inmaculada.Coma@uv.es>
e-Government
Francisco López Crespo (MAE), <flc@ati.es>
Sebastiá Justicia Pérez (Diputació de Barcelona) <sjusticia@ati.es>
Free Software
Jesús M. González Barahona (GSYC - URJC), <jgb@gsyc.es>
Israel Herráiz Tabernero (Universidad Politécnica de Madrid), <isra@herraiz.org>
Human-Computer Interaction
Pedro M. Latorre Andrés (Universidad de Zaragoza, AIPO), <platorre@unizar.es>
Francisco L. Gutierrez Vela (Universidad de Granada, AIPO), <fgutierr@ugr.es>
ICT and Tourism
Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga), <{aguayo, guevara}@lcc.uma.es>
Informatics and Philosophy
José Angel Olivas Varela (Escuela Superior de Informática, UCLM), <joseangel.olivas@uclm.es>
Roberto Feltrero Oreja (UNED), <rfeltrero@gmail.com>
Informatics Profession
Rafael Fernández Calvo (ATI), <rfcalvo@ati.es>
Miquel Sárries Griñó (ATI), <miquel@sarries.net>
Information Access and Retrieval
José María Gómez Hidalgo (Optenet), <jmgomezh@yahoo.es>
Manuel J. Maña López (Universidad de Huelva), <manuel.mana@diesia.uhu.es>
Information Systems Auditing
Marina Touriño Troitiño, <marinatourino@marinatourino.com>
Manuel Palao García-Suelto (ATI), <manuel@palao.com>
Knowledge Management
Joan Baiget Solé (Cap Gemini Ernst & Young), <joan.baiget@ati.es>
Language and Informatics
M. del Carmen Ugarte García (ATI), <cugarte@ati.es>
Law and Technology
Isabel Hernando Collazos (Fac. Derecho de Donostia, UPV), <isabel.hernando@ehu.es>
Elena Davara Fernández de Marcos (Davara & Davara), <edavara@davara.com>
Networking and Telematic Services
José Luis Marzo Lázaro (Univ. de Girona), <joseluis.marzo@udg.es>
Juan Carlos López López (UCLM), <juancarlos.lopez@uclm.es>
Object Tecnology
Jesus García Molina (DIS-UM), <jmolina@um.es>
Gustavo Rossi (LIFIA-UNLP Argentina), <gustavo@sol.info.unlp.edu.ar>
Personal Digital Environment
Andrés Marín López (Univ. Carlos III), <amarin@it.uc3m.es>
Diego Gachet Páez (Universidad Europea de Madrid), <gachet@uem.es>
Real Time Systems
Alejandro Alonso Muñoz, Juan Antonio de la Puente Alfaro (DIT-UPM),
<{aalonso,jpuente}@dit.upm.es>
Robotics
José Cortés Arenas (Sopra Group), <joscorare@gmail.com>
Juan González Gómez (Universidad cARLOS III), <juan@iearobotics.com
Security
Javier Areitio Bertolín (Univ. de Deusto), <jareitio@deusto.es>
Javier López Muñoz (ETSI Informática-UMA), <jlm@lcc.uma.es>
Software Engineering
Javier Dolado Cosín (DLSI-UPV), <dolado@si.ehu.es>
Daniel Rodríguez García (Universidad de Alcalá), <daniel.rodriguez@uah.es>
Students' World
Federico G. Mon Trotti (RITSI), <gnu.fede@gmail.com>
Mikel Salazar Peña (Area de Jovenes Profesionales, Junta de ATI Madrid), <mikeltxo_uni@yahoo.es>
Technologies and Business
Didac López Viñas (Universitat de Girona), <didac.lopez@ati.es>
Francisco Javier Cantais Sánchez (Indra Sistemas), <fjcantais@gmail.com>
Technologies for Education
Juan Manuel Dodero Beardo (UC3M), <dodero@inf.uc3m.es>
César Pablo Córcoles Briongo (UOC), <ccorcoles@uoc.edu>.
Technological Trends
Alonso Álvarez García (TID), <aad@tid.es>
Gabriel Martí Fuentes (Interbits), <gabi@atinet.es>
University Computer Science Teaching
Cristóbal Pareja Flores (DSIP-UCM), <cpareja@sip.ucm.es>
J. Ángel Velázquez Iturbide (DLSI I, URJC), angel.velazquez@urjc.es>
Web Standards
Encarna Quesada Ruiz (Virati), <encarna.quesada@virati.com>
José Carlos del Arco Prieto (TCP Sistemas e Ingeniería), <jcarco@gmail.com>

Copyright
© ATI 2013
The opinions expressed by the authors are their exclusive responsibility

Editorial Office, Advertising and Madrid Office
Plaza de España 6, 2ª planta, 28008 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Layout and Comunidad Valenciana Office
Av. del Reino de Valencia 23, 46005 Valencia; Tlfn. 963740173 <novatica_prod@ati.es>
Accounting, Subscriptions and Catalonia Office
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>; <novatica.subscripciones@atinet.es>
Aragon Office
Lagasca 9, 3-B, 50006 Zaragoza Tlfn./fax 976235181 <secreara@ati.es>
Andalucía Office <secreand@ati.es>
Galicia Office<secregal@ati.es>
Advertising Plaza de España 6, 2ª planta, 28008 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Legal deposit: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Cover Page: Dancing House - Concha Arias Pérez / © ATI
Layout Design: Fernando Agresta / © ATI 2003

Special English Edition
2012/2013 Annual Selection of Articles

summary

editorial

Novática: Reaching beyond International Borders > 02
Dídac López Viñas, President of ATI

From the Chief Editor´s Pen

Privacy: Our Contribution to a High-Level Debate in the Digital Age > 02
Llorenç Pagés Casas, Chief Editor of Novática

monograph

Privacy and New Technologies
Guest Editors: Gemma Galdon Clavell and Gus Hosein

Presentation. Privacy, Technology and Policy: Social Networks, Data Mining and Surveillance > 04
Gemma Galdon Clavell, Gus Hosein

Privacy and Surveillance Primer > 11
Aaron Martin

European Data Protection and the Haunting Presence of Privacy > 17
Gloria González Fuster, Rocco Bellanova

Secrecy Trumps Location: A Short Paper on Establishing the Gravity of Privacy Interferences Posed by Detection Technologies > 23
Mathias Vermeulen

Surveillance Technology and Territorial Controls: Governance and the 'Lite Touch' of Privacy > 26
Darren Palmer, Ian Warren

Google: Navigating Security, Rights to Information and Privacy > 32
Cristina Blasi Casagran, Eduard Blasi Casagran

Human Traces on the Internet: Privacy and Online Tracking in Popular Websites in Brazil > 37
Fernanda Glória Bruno, Liliane da Costa Nascimento, Rodrigo José Firmino, Marta M. Kanashiro, Rafael Evangelista

Social Networks and the Protection of Personal Information. When Privacy Is Not Perceived As a Right > 44
Massimo Ragnedda

Privacy and Body Scanners at EU Airports > 49
Joan Figueras Tugas

Secrecy Trumps Location: A Short Paper on Establishing the Gravity of Privacy Interferences Posed by Detection Technologies

Mathias Vermeulen
European University Institute, Florence (Italy)

<mathias.vermeulen@gmail.com>

Abstract: *Since 9/11 the use of detection technologies has been increasingly seen as a crucial tool to counter terrorism. The use and deployment of these tools more often than not poses an interference with the right to privacy, including tools that are used in public places. In this contribution we will claim that the location where a privacy intrusive measure takes place is less of a determinant to establish the intrusiveness of a measure to the core of the right to privacy than the secrecy of such a measure.*

Keywords: *Detection Technologies, GPS, Human Rights Law, Privacy, Secrecy.*

Author

Mathias Vermeulen is a Research Fellow at the Law Faculty of the European University Institute (EUI) in Florence and a part-time researcher at the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB).

1. Introduction

According to the European Commission, the term 'detection technology' can refer to almost anything "*used to detect something in a security or safety context, with the focus on law enforcement, customs or security authority*"[1].

Recently the EU counter-terrorism coordinator stressed the importance of detection technologies that enabled the investigation of IT services, the interception of telecommunications and the use of tracking devices (or other recording equipment) placed underneath or inside vehicles moving within the territory of several Member States. According to the EU counter-terrorism Coordinator the "terrorism phenomenon" is now "so specialized" that "*it can often be detected only with relatively sophisticated investigative techniques*"[2].

The message that new technologies are needed to counter new threats of terrorism is not a new one. Thirty years ago the European Court of Human Rights (ECtHR) already stated the following: *Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction.*[3]

Little seems to have changed in the last 30 years: surveillance through the use of new technologies continues to be seen as a vital tool to prevent terrorist attacks.

At the same time concerns persist that these detection technologies threaten or violate the right to privacy. The European Court of Human Rights has developed a set of minimum safeguards regarding the use of specific detection technologies that are used in secret to intercept communications, but recently ruled in the Uzun case[4] that those safeguards are not applicable to secret surveillance with a GPS-device that tracked the movements of a suspect.

This contribution disagrees with that position, and argues that the principal factor determining the gravity of interference with the core of the right to privacy is not whether a technology detects the locations, movements or expressions of persons, but whether it does so secretly.

2. The Core of the Right to Privacy

Determining which elements of the right to privacy represent the 'core' of the right to privacy, or, in other words, are 'essential' is not a merely theoretical issue; it should affect the development, deployment and use of specific detection technologies. In X and Y vs. The Netherlands the Court for instance has indicated that the nature of the State's obligation to protect a right will depend on the particular aspect of private life that is at issue. In a case where "*essential aspects of private life are at stake*" the margin of appreciation is lower[5]. Addressing issues related to the protection of personal data will not suffice to determine the limits of the use of detection technologies. In this context the right is predominantly procedural: it informs the right to privacy and provides important parameters of control over some aspects of the private life of a person[6].

The inviolable core of a right is a sub-category of a human right that is applied in an absolute fashion, so that within its scope of application, this core determines the outcome of the case, irrespective of any other legal arguments made. A right can carry more than one core, i.e. more specific norms to be categorized as a rule[7].

In the case of privacy for instance, it could be argued that there exist at least two "core" areas. The first part relates to the 'essential' core of "pure privacy" and is similar to the *forum internum* dimension of freedom of religion, which refers to the internal and private realm of the individual against which no state interference is justified in any circumstances[8]. Similarly, the *forum internum* dimension of the right to privacy could consist of the right of an individual to own his/her own identity, or identities, including the right to change and not to disclose these identities.

A concrete aspect of this *forum internum* element of the right to privacy includes the freedom to express one's most intimate feelings or sexuality. In Germany the *Bundesverfassungsgericht* developed this element of the core of the right to privacy in a case regarding 'acoustic surveillance'. In this case the Court ruled that every act of surveillance has to be interrupted if there are indications that the surveillance will affect, inter alia, expressions of "innermost feelings or sexuality"[9].

The second part of the core of the right to privacy focuses on its social value: its capacity to protect other human rights, including their core areas on the one hand and its enabling function for the enjoyment of other rights on the other. The right to privacy serves as a basis for other fundamental freedoms, such as freedom of expression, freedom of religion, freedom of association or freedom of movement. Without privacy these other freedoms would not be effectively developed and enjoyed[10].

Interferences with the core of privacy lead to the infamous 'chilling effect', which is detrimental to democracy because it results in self-censorship in expressing deviant beliefs and inhibitions from doing 'unconventional' things. Interferences with this core of privacy threaten not only these activities, but also – in the words of Jeffrey Rosen "*gradually dampen the force of our aspirations to it*"[11].

> "In the case of privacy for instance, it could be argued that there exist at least two "core" areas. The first part relates to the 'essential' core of "pure privacy" and is similar to the *forum internum* dimension of freedom of religion"

The right to privacy in this context functions primarily as a limit to the power of the state. Seen from this perspective it can be argued that the location where a privacy intrusive measure takes place is less of a determinant to establish the intrusiveness of a measure to the core of the right to privacy than the secrecy of such a measure.

Jeremy's Bentham's design for a Panopticon showed this already in 1791: being aware of the possibility of surveillance is just as inhibitory as actual surveillance[12]. Or, as Solove more recently highlights: "*In fact, there can be an even greater chilling effect when people are generally aware of the possibility of surveillance, but are never sure if they are being watched at any particular moment*"[13].

3. Challenges Posed by Secret Interferences with the Right to Privacy

The European Court of Human Rights has highlighted the threat of secret interferences with the right to private life in its case law under Article 8[14].

There are a number of reasons for this. The risk of arbitrariness in interferences with the right to privacy is greater when a power of the executive is exercised in secret[15]. Since secret measures take place without the knowledge of the individual who has been put under surveillance, seeking an effective remedy against this interference is rendered more difficult or even prevented. Often the individual concerned cannot take a direct part in any review proceedings of the interference either[16]. The Court has noted that this has an impact beyond the individual. In such a context, "*widespread suspicion and concern among the general public that secret surveillance powers are being abused*" would not be unjustified according to the Court[17]. In view of the risk of abuse intrinsic to "*any system of secret surveillance*", the Court has claimed that any such system "*must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated*"[18].

It seems to be undisputed that the only legitimate secret use of detection technologies can be in the context of the investigation or prevention of serious crime.

The European Court of Human Rights has stated for instance that secret telephone tapping is a "*very serious interference*" with a person's rights and that "*only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorizing it*"[19].

It further indicated that the secret surveillance of citizens is only tolerable in so far as it is strictly necessary for safeguarding the democratic institutions, because a system of secret surveillance to protect national security entails the risk of "*undermining or even destroying democracy on the ground of defending it*"[20].

The European Court of Human Rights developed a strict set of minimum safeguards that should be set out in statute law in order to avoid abuses of power in cases of secret measures of surveillance: the nature of the offences which may give rise to the surveillance; a definition of the categories of people liable to be under surveillance; a limit on the duration of the surveillance; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the data should be deleted[21].

4. New Tools, New Challenges? GPS Trackers as 'Public' Detection Technologies

While the European Court of Human Rights has developed a set of minimum safeguards regarding the use of specific detection technologies that are used in secret to intercept communications, the Court recently said that these specific minimum safeguards which are to be set out in statute law are not applicable to secret surveillance with a GPS-device[22], because secret surveillance with such a device is considered to interfere less with a person's private life than, for instance, telephone tapping[23].

The Court said that GPS surveillance: "*by its very nature*" is to be distinguished from "*other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings*"[24].

The Court missed a chance here to fine-tune the right to privacy in the 21st Century. The Court did not take into account here the emerging importance of the concept of locational privacy, which may be defined as the ability of an individual to move in public spaces with the expectation that their location will not normally be systematically and secretly recorded for later use[25]. In the words of Beresford and Stajano, locational privacy is "*the ability to prevent other parties from learning one's current or past location*"[26].

This concept is increasingly important as location data from GPS and mobile phones allow for the localization of an individual on a much wider scale, thereby enabling the correlation of individual behaviour to objects, places and other individuals[27].

Besides these two most important providers of location data (GPS and mobile phones), there are also a number of other techniques with which location information can be generated, including RFID (*Radio Frequency IDentification*) and biometric applications[28]. All this location data can paint a picture of the user's communication behaviour, of his actions, whereabouts or movements, which can reveal details about personal profiles, relationships, and other aspects of personal life that would not ordinarily be observed by others.

Secret surveillance of location data should therefore not "by its very nature" be distinguished from visual surveillance. The secrecy of the measure makes it potentially equally threatening for the core of the right to privacy. Nowadays such surveillance for a prolonged period of time is able to disclose just as much information about a person's conduct as an intercepted phone call, and the monitoring of such movements has an equally chilling effect on the enjoyment of other rights.

The argument above does not prevent one from arguing that the secret surveillance of personal expressions either by speech or text is a more serious interference with the core of the right to privacy. But it is unfortunate that the court chose not to apply the strict *Weber and Saravia* standards to the use of GPS trackers. The principal factor determining the gravity of interference with the core of the right to privacy is not whether a technology detects the locations, movements or expressions of persons, but whether it does so secretly. The distinction between detecting movements and

> "It seems to be undisputed that the only legitimate secret use of detection technologies can be in the context of the investigation or prevention of serious crime"

detecting expressions should come in only as a secondary step.

5. Conclusion

This short paper argues that detection technologies that are used in secret constitute the gravest interference with the core of the right to privacy; the distinction between detecting (public) movements and (private) expressions should only come in as a secondary step to determine the gravity of the interference with the right to privacy. Secret surveillance of location data should not by their "very nature" be distinguished from visual surveillance; they can reveal equally sensitive information and Courts should therefore attach as much importance to the procedural safeguards that are attached to the latter type of surveillance.

Notes

[1] COM (2006) 474, p.19.
[2] EU Counter-Terrorism Coordinator, Judicial dimension of the fight against terrorism – Recommendations for action, Doc 13318/1/10, 28 September 2010, at 3.
[3] European Commission on Human Rights. Klass and others v. Federal Republic of Germany, Application No. 5029/71, 1977, at para. 48.
[4] European Court of Human Rights, Fifth Section. Case of Uzun v. Germany (Application no. 35623/05), <http://ius.unibas.ch/fileadmin/user_upload/fe/file/EGMR_Uzun_v._Germany__2010_.pdf>.
[5] European Commission on Human Rights. X and Y v. The Netherlands, Judgment of 26 March 1985, para. 24-27.
[6] For a broader discussion see Paul De Hert, Serge Guthwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalism in action", in Serge Gutwirth, Yves Poullet, Paul De Hert, J. Nouwt, C. De Terwangne (eds.) "Reinventing data protection?" Springer Science, Dordrecht, 2009, pp. 3-44.
[7] **Martin Scheinin.** Terrorism and the pull of 'balancing' in the name of security, in Martin Scheinin (ed.), Law and Security - Facing the dilemmas. EUI Law Working Paper 2009/11, 2009, at 55.
[8] CCPR/C/21/Rev.1/Add.4, General Comment No. 22: the right to freedom of thought, conscience and religion, 30 July 1993, par.3.
[9] **G. Hornung, C. Schnabel.** Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention, Computer Law & Security Review 25, nr. 2 (2009): p. 117.
[10] **Martin Scheinin.** UN Doc. A/HRC/13/37, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 28 December 2009, para. 33 .
[11] **Jeffrey Rosen.** The Naked Crowd: Reclaiming Security and Freedom in an anxious age. London, Random House (2004), p.36.
[12] "*The Panopticon is a type of institutional building designed by English philosopher and social theorist Jeremy Bentham in the late 18th century. The concept of the design is to allow a watchman to observe (-opticon) all (pan-) inmates of an institution without them being able to tell whether or not they are being watched*". <http://en.wikipedia.org/wiki/Panopticon>.
[13] **Daniel Solove**. A taxonomy of privacy, University of Pennsylvania Law Review 154, nr. 3 (January 2006): p. 495.
[14] See most recently ECtHR, Weber and Saravia v. Germany, Application no. 54934/00 (Admissibility Decision) (2006)., par. 93; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application no. 62540/00 (2007), par. 75; Liberty and Others v. the United Kingdom, Application no. 58243/00, (2008) par.62; and Iordachi and Others v. Moldova, Application no. 25198/02, (2009), par.39.
[15] ECtHR, Bykov v. Russia (Application no. 4378/02),(2009) para. 78; Huvig v. France, Application no. 11105/84, (1990), at 29-32.
[16] See also European Commission on Human Rights, Klass and others v. Federal Republic of Germany, Application No. 5029/71. (1977), para. 52.
[17] ECtHR, Kennedy v. The United Kingdom (Application no. 26839/05) (2010), para.124.
[18] See ECtHR, Kopp v. Switzerland, Application n° 13/1997/797/1000,(1998) at 72; Weber and Saravia v. Germany, Application no. 54934/00 (Admissibility Decision) (2006), para. 93.
[19] ECtHR. Iordachi and others v. Moldova, Application no. 25198/02 (2009), para. 51.
[20] European Commission on Human Rights. Klass and others v. Federal Republic of Germany, Application No. 5029/71 (1977), para. 49.
[21] ECtHR. Weber and Saravia v. Germany, Application no. 54934/00 (Admissibility Decision) (2006), para. 95.
[22] ECtHR. Uzun v. Germany (Application no. 35623/05) (2010), para. 66.
[23] Idem. para. 72.
[24] Idem, para. 52.
[25] **Andrew J. Blumberg, Peter Eckersley.** "On Locational Privacy, and How to Avoid Losing it Forever" (Electronic Frontier Foundation, August 2009), p. 2.
[26] **A.R.Beresford, F. Stajano.** "Location Privacy in Pervasive Computing". IEEE Pervasive Computing, 2(1), pp. 46-55.
[27] **Ronald Leenes.** Mind my step?, TILT Law & Technology Working Paper Series, nr. 011 (2009): p. 6.
[28] Nouwt, ibid. note 22, at 381.