The King's Student Law Review

Reconciling Privacy and Right to Information in Electronic Access to Court Records

Author: Talia Schwartz Maor

Source: *The King's Student Law Review*, Vol. 7, No. 2 (2016), pp. 76-101

Published by: King's College London on behalf of The King's Student Law Review

---

KSLR is an independent, not-for-profit, online academic publication managed by students of the King's College London School of Law. The *Review* seeks to publish high-quality legal scholarship written by undergraduate and graduate students at King's and other leading law schools across the globe. For more information about KSLR, please contact info@kslr.org.uk

Reconciling Privacy and Right to Information in Electronic Access to Court Records

*Talia Schwartz Maor**

The principle of open-door judiciary is not new, yet its manifestation in the Information era, in which traditional legal practices transform into their e-versions, brings a new set of open ended questions that challenge the boundaries of existing legal norms. This paper explores one aspect of Open Justice – court record's accessibility. Specifically, the paper focuses on the transition from physical access to an electronic, remote access. It analyses electronic access to legal decisions and examines the ever present tension between the right to privacy and accessibility. The paper contributes to the ongoing dialogue on open judiciary by asking the following questions: (1) How does electronic-remote access to court records differ from physical access? (2) What is the legal basis for public access and transparency? (3) What are the benefits and risks of electronic access? (4) How do current legal arrangements and open justice initiatives differ from one another? (5) How does the dynamics between privacy and right to information shape current practices? In offering a limited comparison between two legal systems, Common Law and Civil Law, the paper finds that legal arrangements of electronics access to court records are driven by social preferences and traditional perceptions of justice in a given society. Building up on an established theoretical framework, the paper suggests a paradigm that considers privacy and access as values that go hand in hand in the open justice era. Looking at the question of electronic access to court records through the lenses of reconciling the right privacy and information, the conflict model and balancing test are mitigated with an aggregate, holistic approach.

Introduction

Cyber sceptics argue that the Internet has changed nothing and that Open Judiciary is hardly a novel concept. Rather, electronic access to court records is merely a natural evolutionary stage of our justice systems. Public records, and court records among them, have always been transparent and should be kept as such given that the principles behind public access to judicial proceedings, physical or virtual, remain. Such a simplistic vantage point posits that the digital age simply calls for broadening the scope of traditional access so that it encompasses *digital* access to court records. Yet, substantial differences between online and physical retrieval of legal information cannot be ignored, and as such, signals a reconsideration of the guiding principles on electronic access to court records.[1] As stated by the Justice Brennan in *Whalen v. Roe*,

> Obviously…collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional *simply* because new technology makes the State's operations more efficient… [*Yet*] The central storage and easy accessibility of computerized data vastly increases the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.[2]

Later in the *Reporters Committee for Freedom* case, the Supreme Court stated that, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[3] A study by

---

* JSD Berkeley Law (Expected 2018).

[1] Daniel J. Solove, 'Access and Aggregation: Privacy, Public Records, and the Constitution' (2002) 86 MINN. L. REV. 1137 [Arguing that current systems do not provide enough protection for privacy, where, considering the transition to online access, there exists a much greater risk for commercialization or other exploitation of individual's private information.]

[2] *Whalen v. Roe* [1977] 429 U.S. 589 [In that case the US Supreme court applied a delicate balance between one's privacy right and public interests, and held that the government is entitled to collect personal health information for the purposes of maintaining public health and safety, so long as the information will be kept confidential. In his ruling, the court asserts that given its sensitivity, personal health information is a protected category under a constitutional right to information privacy. The court also places an emphasis on the fact that the database at hand is computerized, noting both the type of information collected as well as the means throughout which it was gathered.]

[3] *United States Department of Justice v. Reporters Committee for Freedom of the Press* [1989] 489 U.S. 749, 764 [In this case, a news channel requested the FBI to disclose "rap sheets" containing arrest and conviction records on millions of people, arguing that the released to the public is mandatory under The Freedom of Information Act (FOIA), 5 U.S.C. § 552. The Supreme Court held that while the data is generally subject to FOIA disclosure rules, in balancing personal privacy and the public's interest in access, an agency (FBI) may "categorically" weigh these values and disclose only records that are informative on the operations of government, that thus constitute a genuine

Nissenbaum et al. cited multiple differences between online and physical access. These differences include the significant added cost to physical access, as well as significant added difficulties in linking multiple information sources when conducting a physical search.[4] Aside from these empirical findings, there are theoretical differences between the virtual domain and physical one. These differences force policy makers and academics to rethink and define an "electronic open doors" principle. For example, statutes of limitations on judgments lose their meaning in light of the Internet's eternal capacity. The ability to start over, to rehabilitate, is more limited given the Web's endless memory. With 'the right to be forgotten' being debated world-wide, it is now clear that a person sitting in a court room listening to a trial (or reviewing papers that relate to it) is subjected to human limitations that the computer does not suffer from, making physical open doors inherently a much narrower right.

Indeed, the argument that online access to court records "is merely an administrative move towards greater efficiency"[5] seems to have been neglected by the majority of legal scholars[6], considering the death of 'practical obscurity'[7] online. 'Practical obscurity' is well described by Peter Winn who states, "Paper records—like human beings—are organic", thus undergo a

---

public interest in their release. It should be noted however that the balancing test applied by the court is applicable only to FOIA cases that explicitly applies only to the executive branch.]; Similar view is reflected in courts in the US agreeing that while the constitution grants the right to attend judicial proceedings, it does not allow the same protection for the right to access judicial documents. See Amanda Conley, Anupam Datta, Helen Nissenbaum and Divya Sharma, 'Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry' 71 MD. L. REV. 772, 776 and references there, in particular to *Zenith Radio Corp. v. Matsushita Elec. Indus. Co*., [1981] 529 F. Supp. 866, 897 (E.D. Pa. 1981) [In which the court held that access to court records does not equal the right to attend proceeding, whereas the former is not protected by the constitution.]

[4] Nissenbaum, Ibid, at 821-824 [describing cost differences in online versus physical access to court records resulting inter alia from added to costs of commuting to the information system, a costlier access restriction mechanism at courthouses and as human factors in physical search requires the involvement of additional personal and court employees.]

[5] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 WASH. L. REV. 119, 120-121 [further stating that "Nothing has changed, fundamentally."]; Helen Nissenbaum, *Privacy in Context. Technology, Policy, and the Integrity of Social Life* (Stanford Law Books 2010).

[6] An important critique is offered by Hartzog and Stutzman, in their attempt to revive online obscurity. See Woodrow Hartzog and Frederic D. Stutzman, 'The Case for Online Obscurity' (2013) 101 CAL. L. REV. 1 [Pointing to empirical research that demonstrates that Internet users rely mainly on obscurity to protect their privacy, arguing that obscurity is a critical component of online privacy. And yet authors do acknowledge that the lack of clarity as to the definition of obscurity has resulted in courts and lawmakers overlooking it].

[7] Arminda Bradford Bepko, 'Note, Public Availability or Practical Obscurity: The Debate Over Public Access to Court Records on the Internet' (2005) 49 N.Y.L. SCH. L. REV. 967, 968; Nancy S. Marder, 'From "Practical Obscurity" to Web Disclosure: A New Understanding of Public Information' (2009) 59 SYRACUSE L. REV. 441; Snyder, D. L. Nonparty, 'Remote Electronic Access to Plea Agreements in the Second Circuit' (2008) 35 Fordham Urb. L.J. 5, 1266-1267

"natural progression of decay and change".[8] Paper is mortal, electronic pages are simply not. The transition from paper-based to electronic information system – a system not bound to temporal or physical constraints – impacts a broad range of socio-legal concerns far beyond court records. Similar debates are ongoing with regard to electronic access to financial data and health care records, although these informational categories receive greater legislative attention.[9]

The importance of this paper's topic – the transition to online access to court records – results from the new set of questions it raises, specifically with reference to the tensions between individual rights and long-lasting legal traditions in the virtual realm; while the normative commitment to transparency was and is still the underlying issue, the manner in which information flows has clearly changed, possibly changing the debate's entire context.[10] The paper objectives are two fold; first, it highlights the impact of the transition to online access compared with traditional "open door" principle by exploring the concerns revolving online access, mainly focusing on the inevitable conflict between transparency and the right to privacy in that digital context. Second, the paper provides an analysis of these counter-values by establishing the relevant theoretical framework as well as providing two case studies of electronic access to court records in practice, in a Common Law and a Civil Law legal system. It suggests that striking the right balance between the competing interests requires abandoning a dichotomous "either or" approach, and replacing it with a contextual paradigm, accompanied by tailor made solutions.

The paper unfolds as follows. Part I provides an introduction to terminology and an overview over open justice initiatives granting electronic access to court records. Part II lays out the normative framework for both the principle of publicity and the right to privacy in the digital age. Leading theories on privacy, such as from Warren and Brandeis, Ruth Gavison, Helen

[8] Peter A. Winn, 'Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information' (2004) 79 WASH. L. REV. 307, 316 [Examining the traditional balance between openness and counter-values in US case law. Generally, Winn finds that that courts in the U.S. are likely to rule in favour of public right of access when it is consistent with ensuring the credibility of the judicial system – and are likely to protect individual's privacy interests when access to personal information bears little relationship to ensuring the integrity of the judicial process.]

[9] Winn, n 8, at 317-318

[10] Nissenbaum, n 3, at 807, 827 [Stating a "widespread agreement that the choice of medium makes a difference to degree of access"]; See also Nissenbaum, n 5, at 152 [Describing that the change in placement has altered the range of accessibility from local to global and the possible implication of that change.]

Nissenbaum, Daniel Solove and Richard Posner, are contrasted. Part III offers a limited comparative view on electronic access to court records by comparing Australia and France as polarized case studies on an "openness" spectrum, ranging respectively from highly open access to a fairly restricted one. Lastly, Part IV concludes by suggesting the rethinking of the governing paradigm of dichotomy, and proposes a framework of reconciling privacy and the accessibility in the digital era.

I. Overview on Open Justice initiatives

There are several categories of judicial information within access to court records. Firstly, adjudicative work of courts ('pure' legal text) differs from information of an administrative or organizational nature as well as data about judicial practitioners (i.e., judges, clerks, and court employees.) Secondly, method of classification refers to the categories of legal documents themselves as used in different stages of the legal proceeding, including forms of complaint, briefs, depositions, evidence, etc.[11] For the purpose of this paper, the term "court records" or "judicial information" refer to the most basic unit of legal data, which is – a court decision.

Court decisions are available in most countries in various information retrieval systems. Three main categories need to be addressed when considering Open Justice initiatives – legal information institutes, privately held legal databases, and government databases. The latter are a common practice in the vast majority of countries across the globe, yet these databases greatly differ from one another in their method of operation, cost, and scope. Such information systems include PACER in the United States[12] and Legifrance in France.[13] Moreover, Legal Information Institute (LII) can be found in a growing number of countries. LII is mostly an independent, non-profit research facility. Some examples include AustLII, the Australasian legal databases; CanLII in Canada; AsianLII, Asian Legal Information Institute; African Legal Information Institute, AfricanLII; Cornell Legal Information Institute and CourtListener in the United States; The

[11] Nissenbaum, n 3, at 778-784

[12] An electronic public access system provided by the United States judiciary <https://www.pacer.gov> accessed 25 April 2016

[13] French government entity responsible for publishing legal texts online <http://www.legifrance.gouv.fr/Traductions/en-English> accessed 25 April 2016

British and Irish Legal Information Institute BAILII.[14] The third type of legal databases is privately held and typically require a subscription fee or other form of direct pay, for example, Westlaw in the United States and Takdin in Israel. Additionally, Google scholar Case law collection is somewhat of a hybrid between the above discussed options, as it is a privately held, yet free of charge database, that indeed marks a "move beyond making law *available* on the Web to making it truly *accessible* on the Web."[15]

The classification of legal databases into various types according to technological criteria and business model is critical given these variables' impact on balancing privacy and access. Generally, a database held by private for profit actors, utilizing open access platform, provides a higher level of access and greater potential harm to privacy. Table 1 analyses the level of access and privacy impact, depending on the database type.

Database type	**Level of access**	**Privacy impact**
By case name	Partial	Low
Designated legal databases	Full	Medium
Open access databases	Full	High
Following anonymization	Almost full	Low

Israel Digital Rights Movements amicus curiae.[16]

II. Two conflicting rights? The right to information versus the right to privacy

A. Transparency – The right to information and the Open court principle

Publicity is a core principle in the Anglo-American justice system.[17] From Hale in the 17th Century to Blackstone in the 18th, all seem to agree on the paramount nature of transparency in

[14] For a full list of legal information database by country see WorldLII Databases <http://www.worldlii.org/databases.html> accessed 25 April 2016; For an overview of some of these databases see Graham Greenleaf, 'The Global Development of Free Access to Legal Information' (2010) 1(1) EJLT <http://ejlt.org//article/view/17> accessed 25 April 2016

[15] Thomas Bruce, Google Scholar Blog, 'Caselaw is Set Free, What Next?' (October 20, 2014) <http://googlescholar.blogspot.com/2014/10/caselaw-is-set-free-what-next.html> accessed 25 April 2016

[16] Supreme Court of Israel sitting as Supreme Court of Justice 5870/14 *Hashavim H.P.S. Business Information vs. Israeli Court Administration* (amicus curiae brief by Israel Digital Rights Movements.)

the functioning of legal process. Transparency allows auditing and thus limits court's powers, and assures proceedings are conducted fairly.[18] As noted by Bentham, "publicity is the very soul of justice. It is the keenest spur to exertion and the surest of all guards against improbity. It keeps the judge himself while trying under trial."[19] Bentham reasoned that without publicity, all other checks (as recordation and appeal) are insufficient.[20] Justice Burger further articulated this notion, with specific regard to the publicity of criminal proceedings,

> [T]he crucial prophylactic aspects of the administration of justice cannot function in the dark... To work effectively, it is important that society's criminal process satisfy the appearance of justice... and the appearance of justice can best be provided by allowing people to observe it.[21]

The tradition of providing public access to court records in Anglo-American systems is "as longstanding as our right to the courts and to justice itself: it is based on the widely held belief that for a justice system to function successfully and consistently, it must be accountable to its citizens."[22] Scholar Daniel Solove lists four distinct functions of transparency and access to court records: (1) public monitoring over courts functioning; (2) public inspection over public officials; (3) facilitating social transaction, and (4) developing case law as a source of information.[23] The right to access court decisions also derives from the public's ownership over public data. While there not all scholars agree in this regard,[24] the justice system, as a government entity, is funded by the tax payer and is thus 'owned' by and account for the *people*.

---

[17] Solove, n 1, 1153-1155 [Solove sets out a different focal point, stating that as a matter of common law, historically, English courts (and subsequently American courts) recognized the right to inspect government records only in certain, limited, circumstances. Professor Solove does state however, that even under the common law, access to court records as opposed to other public records, was broader.]

[18] Matthew Hale, *The History of the Common Law of England* (1713, University of Chicago Press 1971); William Blackstone, *Commentaries on the Laws of England*, (1891) 372-373; See also Cesare Beccaria, On Crimes and Punishments (1764)

[19] John Bowring, *The Works of Jeremy Bentham* (Edinburgh: William Tait, 1838-1843). Vol 4, 316

[20] Ibid. Vol 7, 524

[21] *Richmond Newspapers, Inc. vs. Virginia* [1980] 448 U.S. 555, 572

[22] Nissenbaum, n 3, at 785 and references there to case law. It should be noted however, that while the American system acknowledges a common law right to access court records, its status as a constitutional right is questionable.

[23] Solove, n 1, at 1170-1772

[24] See for example James B. Jacobs and Elena Laurrauri, 'Are Criminal Convictions a Public Matter? The USA and Spain' (2012) 14 PUNISHMENT & SOC'Y 1, 3–28

This property right perspective leads one to logically conclude that free access to the outcome of a justice system is a property right.[25]

B. The right to privacy in the digital age

The theoretical basis for protecting privacy and the values invested in protecting privacy have been heavily studied. Etymologically, the word privacy comes from *privation* or *deprivation*, meaning, isolation and loneliness.[26] For the purpose of this note, three schools of thought are briefly discussed. First, traditional approaches to privacy are presented, referred to as "Privacy-as-personality." Next two streams of criticism are provided – The Contextual Integrity theory and the Economic Theory on privacy. The former is a, a novel approach to privacy which is context based and free from static private-public boundaries — which makes it more suitable for the digital age. The latter, is provided as a broader criticism towards regulating access to information.

Privacy as Personality – Traditional approaches to privacy

In their seminal work, Warren and Brandeis established the idea that the right to privacy is "a part of the more general right to the immunity of the person, the right to one's personality."[27] Warren and Brandeis route their theory in the property oriented approach, asking to protect an individual in his lands and cattle. Yet the idea that privacy is a critical precondition for self-determination and an inherent part of human dignity,[28] has influenced the entire discourse and

[25] The question of ownership as a justification for access is not discussed at length due to obvious limitations, yet it has a dramatic effect that should not be overlooked. Mainly, it is linked with the type of legal data-base and questions concerning the use of court records for commercial, for-profit purposes. One issue discussed in that context is the legality of non-governmental content providers charging individuals for the removal of certain legal content. See David Kravets, Wired, August 2, 2011, 'Mug-Shot Industry Will Dig Up Your Past, Charge You to Bury It Again' <www.wired.com/2011/08/mugshots/> accessed 25 April 2016; Patrick McGreevy, LA Times, August 4, 2014, 'Calif. Senate seeks to outlaw fees by websites for removing mugshots' <www.latimes.com/local/political/la-me-pc-senate-websites-fees-remove-mugshots-20140804-story.html> accessed 25 April 2016

[26] Richard A. Glenn, *The Right to Privacy: Rights and Liberties Under the Law* (ABC-CLIO 2003) 3

[27] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1980) 4 HAR. L. REV. 193, 205, 207

[28] Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 N.Y.U. L. REV. 962, 971

allowed the theory to metamorphose through doctrinal developments, keeping it relevant in today's[29] information era.[30]

The traditional notion of privacy as means of protecting "inviolate personality"[31] and guaranteeing "the right to be let alone"[32], is also rooted in the principle of privacy as autonomy and secrecy. As described by Alan Westin: "The most serious threat to the individual's autonomy is the possibility that someone may penetrate the inner zone and learn his ultimate secrets… (leaving) him naked to ridicule and shame and would put him under the control of those who knew his secrets".[33]

Privacy has been traditionally linked to the one's negative and positive right to control information. This dual right means one has the ability to act free *from* control and inspection and free *to* control one's self-presentation to another. Ruth Gavison defines the interest in privacy as a concern over accessibility – the extent to which we are known to others; to which others have physical access to us, and the extent to which we are the subject of others attention.[34] Particularly relevant to the topic of this paper, Pound introduced a legal party's right to privacy, stating that an individual "may make that his private personal affairs shall not be laid bare to the world and be discussed by strangers."[35]

The Contextual Integrity Theory

Much of the criticism towards the traditional concept of privacy suggests that by conceptualizing privacy in terms of physical separation, control or secrecy, privacy becomes an ambiguous and

[29] Notably, the United States legal systems' tort privacy law is based on Prosser's work, which was highly influenced by Warren and Brandeis theory. Bearing in mind the rational of protecting individuals against mental harm, Prosser transformed Warren and Brandeis theory into an actionable set of harmful behaviours, resulting in the United States legal systems' tort privacy law. William L. Prosser, 'Privacy' (1960) 48 CAL. L. REV. 383

[30] Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 STAN. L. REV. 1373; Jeffrey Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27

[31] Warren and Brandeis, n 28.

[32] Thomas C. Cooley, *Law of Torts* 29 (2d ed. 1888).

[33] Alan Westin, *Privacy and freedom* (New York: Atheneum, 1967) 33

[34] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 YALE L.J. 421; Joel Feinberg, 'Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution' (1983) 58 Notre Dame L. Rev. 445; Hyman Gross, 'Privacy and Autonomy' in J. Roland Pennock & John W. Chapman (eds.), *PRIVACY: NOMOS XIII* 169 (1971); See also Stanley I. Benn, 'Privacy, Freedom and Respect for Persons', in J. Roland Pennock & John W. Chapman (eds.), *PRIVACY: NOMOS XIII* 1 (1971)

[35] Roscoe Pound, 'Interests of Personality' (1915) 28 HARV. L. REV. 343, 362

illusive term.[36] Critics further advance that dichotomous references to privacy are inappropriate considering substantial technological advancements and waves of voluntary exposition in today's "exhibitory society."[37] In an attempt to overcome the lack of a coherent concept of privacy, leading scholars have recently adopted a broader, context base approach towards understanding privacy.

Nissenbaum's information-centric approach suggests a shift from the governing public-private dichotomy and presents a holistic framework[38]. The information centric approach rejects an *a priori* classification of private versus public information. Rather, Nissenbaum suggests that no information is "totally private or totally public."[39] Instead, according to the theory, there is a united sphere of social interaction in which privacy expectation is defined by context.[40] By relating to various factors, including the nature of the information, its context, and how any changes made within a context might affect the underlying values, this theory analyses privacy in a broader context of specific interactions.[41] Fairly similarly, Daniel Solove offers a novel conceptualization of privacy, according to which privacy is a bundle of related problems that share common traits[42]. In criticizing the traditional discourse of theories as these are either too narrow or too broad, Solove suggests moving away from a strict definition and moving towards a broader definition, referring to privacy as an 'umbrella term.' Under this umbrella term, privacy refers to a set of rules that govern actions related to personal information. In the narrow context

[36] Jed Rubenfeld, 'The Right of Privacy' (1989) 102 HAR. L. REV. 737 (1989) [Criticizing traditional approaches to privacy resulting in a vague concept and accordingly unclear measurements needed in order to protect it.]

[37] Bernard E Harcourt, Digital Security in the Expository Society: Spectacle, Surveillance, and Exhibition in the Neoliberal Age of Big Data (2014). Columbia Public Law Research Paper No. 14-404.

[38] Rather than characterizing privacy as control over personal information, or as the limitation of access to information, the Contextual Integrity Theory sees privacy as "conformance with appropriate flows of information, in turn modelled by the theoretical construct of context-relative (or context-specific) informational norms." Nissenbaum, n 3, at 804

[39] Ibid, Nissenbaum, at 805

[40] Nissenbaum, n 5, at 136-138 [Describing a constant shift from and to private and public spheres, without a clear-cut border between the two spheres. Even more so, the contextual integrity theory holds that there are no two separate spheres of public versus private but rather one world of social interactions and governing norms in which privacy expectation is defined by context.]

[41] Among the elements it enlists, the theory relates to three key elements of information – actors (subjects, senders, and recipients), information types and transmission principles. Nissenbaum, n 5, at 153

[42] Daniel J. Solove, 'Conceptualizing Privacy' (2002) 90 CAL. L. REV. 1087 [In his theory on privacy, Solove gives a broad introduction to the concept of privacy and its evolution. Among its many definitions, privacy relates to the right to be let alone, freedom of thought, control over one's body and information and freedom from government surveillance and other means of intrusion.]; See also Daniel J. Solove. *Understanding privacy* (Harvard University Press 2008)

of privacy and public access, Solove's interpretation of the First Amendment suggests that given the rationale behind transparency, the US Constitutional Right to Information encompasses both the right to access public records – as well as the right to privacy.[43]

Neil Richards calls for abandoning the paradigm of the tension between privacy and free speech and suggests replacing it with a notion of the two complementing each other. "Intellectual privacy" he states, is a new form of generating and expressing ideas in the digital age using advanced technologies that allow constant surveillance. This "intellectual privacy" involves perils to both privacy and free speech, requiring the protection of both altogether.[44] Turning to the United Kingdom, Turl suggests a similar model to replace the private-public dichotomy with a spectrum of circumstances that offers an examination of freedom of information and data protection on a case by case basis.[45]

Economic Theory of Privacy

Law and economic scholars have suggested broader criticism towards regulating access to information by the name of privacy. The approach that "knowledge will forever govern ignorance"[46] is mostly illustrated in Richard Posner's theory on privacy. Put simply, Posner's cost-benefit analysis tells the reader that the right to privacy should be balanced against other's right to unmask deception, while taking into account the benefits of knowledge and the costs of misrepresentation.[47] Posner contends that as a matter of transactional-cost analysis, property right in information should be assigned to those who value it most.[48] Posner's critique is also

[43] Ibid, Solove, 1199 [Stating that the "Constitution does not merely mandate public access to information but also obligates the government to refrain from disclosing personal information."]
[44] Neil M Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015)
[45] Turle, Marcus, 'Freedom of Information and Data Protection Law: A Conflict or a Reconciliation?' (2007) 23 Computer Law and Security Report, 514
[46] Letter from James Madison to W.T. Barry (Aug. 4, 1822), in 9 THE WRITINGS OF JAMES MADISON 103 (Gaillard Hunt ed., 1910).
[47] Richard A. Posner, 'The Right of Privacy' (1978) 12 GA. L. REV. 393 [Noting information concerning past criminal activity in particular, as a type of information that people would want to conceal]; Richard A. Posner, An Economic Theory of Privacy, Regulations (May/June 1978).
[48] An important critique to this cost-benefit analysis is made by Alessandro Acquisti. Acquisti, a leading scholar in the field of economic analysis of privacy, shows in his studies that the fact that individuals are not 'willing to pay' the price for privacy is not necessarily due to rational cost-benefit analysis, but because of, inter alia, market failure and asymmetry between individuals and corporates, misunderstanding and defaults established by interest groups. See Acquisti, Alessandro and Taylor, Curtis R. and Wagman, Liad, The Economics of Privacy (March 8, 2016). Available at SSRN: http://ssrn.com/abstract=2580411

property-oriented, making it similar to Warren and Brandeis' approach to privacy, yet remains distinct. Posner perceives information as property and individuals as 'public goods', arguing that the law should not allow people to control information on themselves and thereby mislead others, more than it allows to do so with regard to other goods. "We think it wrong (and inefficient) that the law should permit a seller in hawking his wares to make false or incomplete representation… but people 'sell' themselves as well as their goods."[49] This view assumes rationality and takes into account the fact that individuals are all conducting background checks anyways in our day to day decision-making. In his Reputation Revolution Theory, Lior Strahilevitz suggests provocatively – and rightfully – that in an era of ubiquitous personal information, a policy that calls for the spread of information should be promoted as a tool for tackling social ills.[50]

C. The competing interests

Despite the strength of a right, no right is absolute. Unrestricted, unfiltered access to court records damages individual's invested interests in privacy, maintaining his identity[51] the right to rehabilitate[52], and to be forgotten. The examination of CourtListner legal database as one case study, it shows that indeed the vast majority of removal requests are based on privacy concerns (40% as indicated in table 2.)[53]

---

[49] Posner, n 47

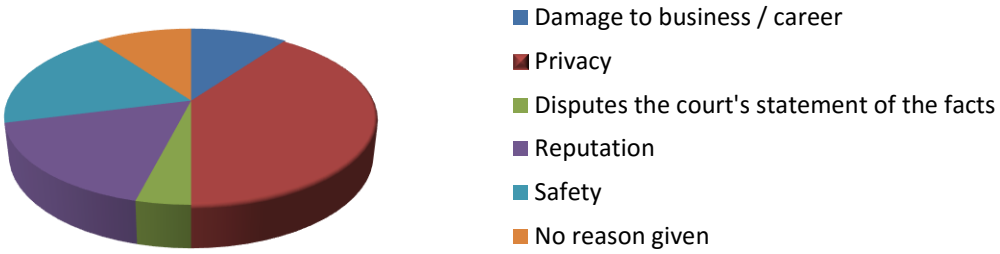
[50] Lior Strahilevitz, 'Reputation Nation: Law in an Era of Ubiquitous Personal Information' (2008) 102 NW. U. L. Rev., 1667, 1679–1682 [The theory points to the fall of anonymity and 'strangeness' and the rise of reputation based markets, and is based on the fact that landlords, employers, and other decision-makers constantly use public information about past criminal records or litigation when evaluating their counterparties.]

[51] Nancy S. Marder, 'From "Practical Obscurity" to Web Disclosure: A New Understanding of Public Information' (2009) 59 SYRACUSE L. REV. 441, 447 [Discussing the risk of identity theft due to the accessibility of highly sensitive data in judicial information.]

[52] See a discussion on the right to rehabilitate in the context of the disclosing information on previous criminal activity in the case of *Briscoe vs. Reader's Digest Ass'n, Inc*. [1971] 483 P.2d 34, 36, 44 [Where the court held that a truthful publication of an eleven-year old conviction constituted a cause of action for invading his privacy, inter alia, due to the individual's right to rehabilitate]; For an initial read on criminal court records and the right to rehabilitate see James B. Jacobs, *The Eternal Criminal Record* (Harvard University Press 2015) [Critiques the easiness in which criminal information is obtained by employers, neighbours and cyber stalkers in the American system, with a particular focus on records of arrests that failed to result in convictions]; Robert A. Brunette, 'Rehabilitation, Privacy and Freedom of the Press—Striking a New Balance: Briscoe v. Reader's Digest Association' (1972) 5 LOY. L.A. L. REV 544 (1972).

[53] Brian Carver, Cornell Legal Information Institute, Putting the Law Online: Balancing Litigant Privacy and Access to the Law, presentation <https://blog.law.cornell.edu/lvi2012/presentation/putting-the-law-online-balancing-litigant-privacy-and-access-to-the-law/ > accessed 25 April 2016

Table 2
CourtListner removal request (reasoning)



Aside from considerations on the individual level, an overly open justice system could potentially have a "chilling effect".[54] The fear from the discloser of sensitive data in legal proceedings could result in individuals turning to alternative, discrete mechanisms, leaving the formal justice system weak and vulnerable. Such reality would create a double standard for privacy, in which individuals are subjected to privacy protection in legal proceedings, depending mainly on their understanding and financial ability. In other words, knowing that legal history might hurt oneself, there may be a potential chilling effect on individual's willingness to turn to courts and their trust in the system.[55] In line with Nissenbaum and Solove's work to change governing dichotomies with regard to privacy, this paper suggests that the conception of privacy in its individualistic context should be coupled with an emphasis on the social value of privacy as well; a school of legal scholars acknowledges an independent public value in protecting privacy. Regan argues for the importance of privacy in maintaining democracy, particularly with regards to protecting individuals against public scrutiny and interference with political decision making.[56] Others argue for the necessity of one's secluded sphere ('a private comfort zone') to maintain public order and social welfare.[57]

---

[54] McGraw D, Dempsey JX, Harris L, Goldman J. 'Privacy as an enabler, not an impediment: building trust into health information exchange' (2009) 28(2) Health Aff (Millwood), 416 [Arguing that protecting the privacy of individual's medical information will enhance people's trust in the system, encourage them to participate in the market and contribute to the healthcare system as a whole.]

[55] Nissenbaum, n 3, at 802 [Stating that sealing court record on certain circumstances "will actually make people more willing and likely to use the system by allaying their fears about the exposure of sensitive personal information or business trade secrets"]; A similar argument driven at large by similar logic is made with regard to user's anonymity online as means of protecting privacy and enabling free participation in the online market of ideas. See Gabriella Coleman, 'Anonymous in Context: The Politics and Power Behind the Mask'. Report for Centre for International Governance Innovation (2013).

[56] Prisicilla M. Regan, *Legislating Privacy. Technology, Social Values, and Public Policy* (1995, UNC Press 2009); The social values of privacy within the meaning of maintaining a democratic political system was also discussed by Julie Cohen. See Cohen, n 30. See also Julie E. Cohen, 'What Privacy Is For' (2012) 126 HARV. L. REV. 1904

On the other hand, the distribution of information is done by the name of free speech,[58] free press, and many other social and national interests.[59] In the judicial context, the traditional notion is that access allows for an informal public scrutiny – monitoring the justice process – "judge the judge".[60] Thus, transparency enhances the public confidence in the justice system. In addition, public access to complete court records also serves a socio-legal function by alerting society of individuals involved in legal proceedings.[61] Moreover, public access creates a deterrence effect that complements the formal judicial sanction. Importantly, one must consider its potential risks of becoming "collective retribution" and a digital form of harassment[62]; the ancient principle of "shaming and blaming" is revived today by reintroducing community's role in the legal process in condemning offenders.[63] For example, in the Netherlands, there is a legislative arrangement allowing the disclosure of parties' names for that exact purpose of social sanction.[64]

From society's point of view, while the risks that open access carries are large, open access also carries potential in a Big Data environment. Digital access to court records in a Big Data era has far reaching applications when considering text analysis methods for example, or other advanced technologies that apply to legal corpus.[65] Such utilisation contributes to a better understanding of

---

[Discussing the value of privacy in terms of self-formation for allowing, inter alia, the flourishing of liberal democracy, particularly in the context of state surveillance.]

[57] Erving Goffman, *The Presentation of Self in Everyday Life* (Unabridged 1959)

[58] Paul M. Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 VAND. L. REV. 1607

[59] One of these interests is national security, whereas in many cases it conflicts with individual's right to privacy. for an overview see Orrin Kerr, 'Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't' (2003) 97 NW. U. L. REV. 607

[60] Karen Gottlieb, 'It Is Public Information, What Is the Problem?' (2004) Swedish Institute of Computer Science - Presentation Using Court Information for Marketing in the United States [For a critique, arguing that the alleged public's right to inspect and examine" and copy for about twenty cents a page" court records originated in the individual right to have an open trial.]

[61] Nissenbaum, n 5, at 152 [justifying the social values of informing the close geographic surroundings of their neighbour criminal record for the purpose of protection against the dangers of recidivism]; See also reference to Megan's Law in the context of individual's privacy in Solove, n 1, at 1147.

[62] Nissenbaum, n 3, at 831 [Noting that there are many other "non-criminals" identified in court records who are subject to the same treatment, including victims, those found innocent, third-parties as witnesses]; A similar differentiation between the innocent and convicted criminal is mentioned in Jacobs, n 52.

[63] One of the leading principles of Problem-Solving Courts approach and community courts is in considering the therapeutic value of the community involvement in the criminal proceeding, whereas social sanction, remorse, and forgiveness are hopefully archives through the social process.

[64] Dutch Code of Criminal Procedure Art. 9(1)(b)(3); Economic Offences Act Art. 7(g). Noting that in there Netherlands there is a widespread anonymization practice which court decisions undergo.

[65] Several examples can be seen in increasing attempts in the academic realm to map court cases in establishing citation networks. See a recent work that identifies anti-mass-incarceration constitutional arguments in case law. Colin Starger, 'Hacking Mass Incarceration', February 15, 2015 <http://blogs.ubalt.edu/cstarger/2015/02/15/hacking-mass-incarceration/> accessed 25 April 2016; See also Smith,

the justice systems. Furthermore, with genealogists analysing court records to trace heritage and learn about forgotten ancestors, access to complete legal information is truly a "part of the common heritage of humanity." Maximizing access to this information promotes justice and the rule of law; public legal information is digital common property, and should be accessible to all on a non-profit basis and free of charge. Organizations such as legal information institutes have the right to publish public legal information, and the government bodies that create or control that information should provide access to it so that it can be published by other parties."[66]

Lastly, examined from the legal party's perspective, despite the general belief that parties to a legal process gain from anonymity, studies show that the mark of a criminal record for example, which has great influence in the labour market for example,[67] might actually benefit those that are less privileged, and are systematically being discriminated against.[68]

III. Practices of electronic access to court records – Common Law versus Civil Law

The governing paradigm of balancing transparency with privacy interests can be demonstrated through justice systems worldwide. In the United States, there is a "customary and constitutionally embedded presumption of openness in judicial proceedings".[69] Openness of criminal proceedings is guaranteed by the Sixth Amendment to the United States Constitution,

---

'The Web of the Law' (2007) 44 SAN DIEGO L. REV. 309; Ruhl, J. B. and Katz, D. M. 'Measuring, Monitoring, and Managing Legal Complexity' (2015) Iowa L. REV. 100; Li, W. Azar, P. Larochelle, D. Hill, P. Cox, J. Berwick, R. C. and Lo, A. W. 'Using algorithmic attribution techniques to determine authorship in unsigned judicial opinions' (2013) 16 STAN. TECH. L. REV. 503

[66] Free Access to Law Movement, Declaration on Free Access to Law, http://fatlm.org/declaration> accessed 25 April 2016.

[67] Devah Pager, 'The Mark of a Criminal Record' (2003) 108 AM. J. SOC. 937, 938 [Noting that about 8% of working aged population in the United States are ex-felons].

[68] Harry J. Holzer et al., 'Perceived Criminality, Criminal Background Checks, and the Racial Hiring Practices of Employers' (2006) 49 J.L. & ECON. 451 [Researchers indicate a widespread discrimination against African Americans males in hiring processes. Strikingly, employers who conducted criminal background checks on applicants were 8.4% more likely to hire African Americans than employers who did not. The study also found evidence that employers who did not conduct criminal background checks used race as a proxy for criminal convictions. As suggested by the authors, "curtailing access to criminal history records may actually harm more people than it helps and aggravate racial differences in labour market outcomes", at 474.]

[69] *Doe vs. Frank* [1992] 951 F2d 320, 323 (11th Cir 1992); Solove, n 1; and also Winn, n 8 [Both providing an in-depth analysis of US case law that illustrate such presumption in favour access.]

which grants each criminal defendant the right to a public trial[70] as well as by the First Amendment's freedom of speech.[71] In the civil context, there is no explicit right to access granted by the constitution, however the US Supreme Court has recognized a common law right to access based on similar rationale for public access to judicial proceedings, *inter alia*, allowing public scrutiny and the proper administration of justice.[72] A leading example for the superiority of the public right to access information over individual's privacy interests can be seen in Megan's Law, federal law, and subsequent state laws in the United States, requiring law enforcement authorities to make information available to the public regarding registered sex offenders.[73] With that said, the American justice system has recognized a Constitutional right to privacy[74], and traditionally, the presumption of openness has been limited in cases it interfered with the administration of justice or other counter-values.[75]

This chapter demonstrates how different jurisdictions determine a different balance point between the right to privacy and the principle of publicity. As illustrated, this balance point is mirrored in the practices surrounding electronic access to court records. Aside from presenting two different legal systems and traditions (Common versus Civil law), Australia and France make particularly interesting case studies given their location on an 'openness' spectrum, ranging from relatively open access to fairly restricted one.

Australia

Accessing court records in Australia is governed by a statutory and common law framework. The Australian Constitution does not define the right of access to judicial information.[76] However,

[70] U.S. Constitution Amendment VI ["In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial"]
[71] Winn, n 8, at 309 and references there to US Supreme Court case *Richmond Newspapers, Inc. v. Virginia* [1980] 448 U.S. 555.
[72] Ibid, at 310 and references there to *Nixon v. Warner Communications, Inc*. [1978] 435 U.S. 589; See also Solove, n 1, at 1196 [Discussing lower court cases granting the right to access court records in civil proceedings.]
[73] For further read on Megan's Law in the context of individuals' privacy see Solove, n 1, at 1147.
[74] For the evolution of the constitutional right to privacy in US courts see Solove, n 1, 1197-1199 [Discussing inter alia, the constitutional right to information privacy that has been evolving ever since the *Whalen* case.]
[75] Winn, n 8, at 308-310 [Describing the various limitations on publicity of criminal proceedings, arguing that many criminal courts are maintained in secrecy, for example, that there is no right of public access to pre-sentence reports and in procedures involving requests for search warrants and for electronic surveillance.]
[76] Sharon Rodrick, 'Open Justice and Suppressing Evidence of Police Methods' (2007) 31 MELBOURNE U. L. REV. 183 [Stating that neither freedom of speech or the right to a fair and public trial are guaranteed in the Australian constitution, in part, due to the belief that individual rights are kept under the protection of common law.]

the system's norm of publicity is inferred from Chapter III of the Constitution which vests judicial power in the courts.[77] Some courts analyse this clause as including "an entrenched requirement of openness".[78] The openness of the judiciary is established as a governing principle in promoting the administration of justice[79]; while Australian courts are not constitutionally bound to open justice (or freedom of expression), the principle is kept through common law norms.[80]

Third parties are required to show sufficient interest to access the *complete* court record, yet media is granted specific authority to inspect any document relating to criminal proceeding for the purpose of a fair report of the proceedings for publication.[81] Different legislative arrangements provide for public access to court administrative records[82] as well as restrict disclosure of sensitive data or prohibit access only in specific circumstances.[83] Australia is one of the first countries to draft a comprehensive legislation that addresses access to court records which includes to electronic access as well. In a recent law,[84] the legislature determined a default of open access,[85] while sketching a line between "open access information" and restricted information (personal identification information.)[86] Given the openness this law promotes, the law lays a responsibility of redacting personal identification information on *courts*,[87] imposing a

[77] Sharon Rodrick, 'Open Justice, the Media and Avenues of Access to Documents on the Court Record' (2006) 29 U.N.S.W.L.J. 90, 117-121

[78] See Solove, n 1, at 1196; Rodrick, n 76, at 187-189 and references there. Again, the broad principle applies here, according to which even a country that does not have a written or common law right of access, the Constitution might be interpreted as requiring a degree of openness.

[79] Ibid, Rodrick [Stating that "Courts have taken the view that the principle of open jus-tice is so fundamental that it can be curtailed only when necessary in the interests of the administration of justice in the particular proceeding."]

[80] Ibid [Suggesting that "the absence of a constitutional imperative has had little impact on the emphasis placed on open justice by Australian courts". Furthermore, the paper describes how Australian courts rarely regard themselves as having power to impose publication bans on judicial proceedings.]

[81] Criminal Procedure Act 1986 (New South Wales), chapter 7 § 314.

[82] See for example Freedom of Information Act 1982, § 5.

[83] Categories of sensitive data relates to victims who are Minor; victims of sexual crimes and data that could impede civil proceedings. Section 11, Children (Criminal Proceedings) Act 1987; § 578A, Crimes Act 1900; § 72, Civil Procedure Act 2005, respectively. Furthermore, the governing framework is that of the Privacy Act 1988 (Cth), drafted in light of the European privacy standard

[84] Court Information Act 2010

[85] Ibid. § 5.

[86] Ibid. part 1 definitions [including the following categories of information: (a) tax file number, (b) social security number, (c) Medicare number, (d) financial account numbers, (e) passport number, (f) personal telephone number, (g) date of birth (other than year of birth), (h) home address (other than suburb, city and State or Territory), (i) other information that can be used to establish a person's identity and that is prescribed by the regulations as personal identification information for the purposes of this Act.]

[87] Id. § 18.

duty to publicize privacy protection measures[88] and taking reasonable security safeguards to protect the data[89]. A party to legal proceedings may access the non-redacted version of the data[90] and the media is entitled for a similar arrangement.[91] Similar to the American framework, a party's name is considered open access information.

France

The legal arrangement on accessing court records under the French regime is influenced largely by European governing framework and the strict European standard for privacy, as reflected *inter alia*, by Article 8 of the European Convention on Human Rights and the Data Protection Directive.[92] Notably, the right to privacy is not explicitly stated in the French Constitution, yet was held by the Constitutional Court as a protected right.[93] Legislation provides open hearing in civil procedures[94], yet the European standard dictates a protection of the "sphere of intimacy" and "private life" [95] of a legal party or third parties.

CNIL[96] is the administrative authority in France responsible for maintaining privacy protection law. With particular regard to electronic access, France Data Protection Act of 1978 defines that information technology shall not violate human identity, including privacy or other liberties.[97] In its decision of 2001,[98] CNIL concluded that the publication of court cases including parties' names in digital legal databases does in fact constitute a processing of personal data in accordance with data protection law. Taking into account the unique and "revolutionary" characteristics of the Internet and online legal databases the commission declared greater caution

[88] Id. § 17.
[89] Id. § 19.
[90] Id. § 11.
[91] Id. § 10.
[92] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[93] Decision 94.352 DC 1994 (*Conseil Constitutionnel*)
[94] Code de Procedure Civile Art. 525 and 783
[95] France's Code de procedure civile Art. 525b and the its definition of "l'intimité de la vie privée".
[96] La Commission Nationale de l'Informatique et des Libertés.
[97] Article 1 of Law No. 78-17 of 6 January 1978 concerning information technology, files and civil liberties, at: www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf.
[98] Decision 01-057 of 29 NOV. 2001 ADOPTING A RECOMMENDATION CONCERNING THE PUBLICATION OF PERSONAL DATA ON THE INTERNET IN CASE LAW DATABASES (Commission nationale de l'informatique et des libertés) <cnil.fr/fileadmin/documents/en/D01-057_decisions%20de%20justice%20VAVF.pdf> accessed 25 April 2016

in protecting individuals' privacy and right to oblivion[99] and adopted the European rule of thumb[100] of complete anonymization.[101] France's Privacy law was amended accordingly, and CNIL was vested with powers to order complete data anonymization as means of securing lawful processing of personal data.[102] The duty to identify and deduct identifiable information is imposed on the data controller. As of 2002 final court decisions go through an automated process of anonymization prior to publication in Legifrance database.[103]

The French default of favouring privacy over open justice through anonymization and the content control (the right to be forgotten) is also revealed in the trial itself. A trial cannot be broadcasted, with many seeking to change this prohibition. There are relatively firm privacy laws (libel laws[104], criminal cause of action and data protection legislation) which naturally result in narrowing the scope of other liberties, for example freedom of expression.[105] The balance point prevailing privacy over conflicting interests in France is encountering difficulties in other aspects

[99] Jeffrey Rosen, 'The Right to Be Forgotten' (2012) 64 STAN. L. REV. ONLINE 88 [French law officially recognizes le droit à l'oubli in 2011, in direct link to court records; the law allows a convicted criminal who has served his time to rehabilitate, and seek the deletion of his criminal record]; According to Google transparency report in 2014, France was the country with the highest number of 'right to be forgotten' removal requests (about 17,500 individual requests involving around 58,000 URLs). Samuel Gibbs, The Guardian, 1 August 2015, 'France requests most 'right to be forgotten' removals from Google' <>www.theguardian.com/technology/2014/aug/01/france-requests-most-right-to-be-forgotten-removals-from-google> accessed 25 April 2016

[100] CNIL report from 2006 state that most European countries anonymize judgments either through national laws (Czech Republic, Estonia, Sweden) or through a privacy protection authorities guidelines (Netherlands, Denmark, Portugal, Lithuania) <www.cnil.fr/fileadmin/documents/approfondir/dossier/police-justice/Bilan_BDD_jurisprudence_decisions_de_justice.pdf> accessed 25 April 2016; See Elena Larrauri, 'Conviction Records in Spain: Obstacles to Reintegration of Of-fenders' (2011) 3 EUR. J. PROBATION 50, 51–52 [Noting the Spanish practice of rendering anonymous decisions and not publishing parties names, except for Constitutional Court decisions]; See also Jacobs and Laurrauri, n 24.

[101] Ibid [stating that "the specific characteristics of the Internet imply to reconsider the balance between the requirement of publicity of judicial decisions and the rights and civil liberties of the persons concerned." Also stating that "The low cost of Internet connections (not to be compared with the cost of Minitel connections), the ease with which information published on the Internet may be duplicated, the impossibility to control the use of this information world-wide, and in particular the use of search engines". Stating also that the "Internet can also be used to find out information about a job applicant, about someone seeking housing or applying for credit, a neighbour or a close relative, and so without the persons in question being aware of it."]

[102] Article 8(III) of Law No. 78-17.

[103] Legifrance database, n 13.

[104] Seth Weintraub, Fortune, 'French Court Convicts Google CEO Eric Schmidt of Defamation', Sept. 26, 2010 <http://fortune.com/2010/09/26/french-court-convicts-google-ceo-eric-schmidt-of-defamation/> accessed 25 April 2016 [Reporting a case in France in which a man successfully sued Google for defamation after Autocomplete terms related to his past criminal record arose in his name search.] See original case (French) Tribunal de Grande Instance de Paris 17ème chambre Jugement du 8 septembre 2010 <www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2985> accessed 25 April 2016

[105] Indexoncensorship, 'France: Strict defamation and privacy laws limit free expression', 19 August, 2013, <https://www.indexoncensorship.org/2013/08/france-faces-restrictions-on-free-expression/> accessed 25 April 2016

such as maintaining security.[106] Specific criticism towards the French anonymization process is also aimed at its automated nature, which at times results in non-personal data deletion that constitutes *de facto* censorship.[107]

The comparison between these two legal systems demonstrates that these jurisdictions find balancing point between the right to privacy and the right to information that is mirrored in the practices surrounding electronic access to court records. Open Justice in Australia, a Common Law jurisdiction, is rooted in the system's core values that 'justice needs to be seen'. France, as a Civil Law jurisdiction, traditionally considers privacy as the leading value. The differences in legal frameworks between the two jurisdiction as they are reflected in open access practices, are the outcome of legal defaults of one right prevailing the other; the French jurisdiction that strongly protect the right to privacy, lean towards imposing more restrictions on digital access (and vice versa.)

Contrasting the two legal systems reveals more than this intuitive observation regarding the differences between legal defaults; it reveals that while the balance point is located at a different point in each case, both Civil and Common Law frame the debate on Open Justice in terms of conflicting interests. Both systems share the paradigm of dichotomy of public interest versus privacy. Both relate to privacy as an *individual* right, whereas access is regarded as part of the *public* right to information. Both see the public right to information *against* the right to privacy as two conflicting rights that needs to be *balanced* against one another.

IV. Reconciling privacy and the accessibility in the digital era

Moving from a governing paradigm of dichotomy to reconciliation

Law is widely held as the science of balancing conflicting interests, led by the notion that no right is ever absolute. Reality forces compromises. Within that framework, privacy and publicity

[106] Kevin Johnson, USA TODAY, February 9, 2015, 'Security vs. privacy: France trying 'to find the line', <www.usatoday.com/story/news/nation/2015/02/09/france-terror-surveillance/23118939/> accessed 25 April 2016

[107] In at least one case such mistake was reported in 2009; a case involved Mattel Corporation, manufacturer of the famous Barbie dolls, names of dolls were omitted in a manner that damaged the ability to read and understand the decision.

are usually regarded as diametric values, with legal scholars, [108] judges and practitioners, going through the "trying task"[109] of finding the proper balance point between the two. Legal traditions come into play when considering the strength of a certain right and the level of protection it is entitled to, thus determining the overall balance point between conflicting rights.[110]

The governing paradigm of countervailing values when discussing electronic access to court records can be demonstrated through justice systems worldwide. As shown, US' strong preference for public access for example, requires substantial privacy concerns to override it.[111] On the other end of the spectrum, some European countries by default seek to protect individuals' privacy rights at the cost of narrowing the scope of other liberties. While different systems define the balance point elsewhere (in part due to influences of Civil versus Common Law norms), they all share a notion of balance.

Yet Open Justice, or the right to electronically access court records, is a legal concept that does not necessarily share a dichotomous structure. It can be regarded as *individual's* freedom of expression or as a *public* right to information. Similarly, the right to privacy is not only of *individual* legal parties, but also has an important public dimension in protecting the justice system as a whole. The evolving nature of information flow in a mixed private-public digital sphere is being debated in a wide range of contexts.[112] The emergence of new forms of communication, information and human behaviour in the digital age requires rethinking pre-Internet traditions and norms, as well as the context of electronic access to court records.

[108] Nissenbaum, n 5, at 151 [Describing the need to pursue trade-offs and balances when the two rights "clash".]
[109] *Bridges v. California* [1941] 314 U.S. 252, 260 [Paraphrasing Judge Black of the United States Supreme Court that stated "free speech and fair trials are two of the most cherished policies of our civilization, and it would be a trying task to choose between them."]
[110] To illustrate that point, one can examine the differences between US "copyrights", the French "droit d'auteur" and the German "Urheberrecht". Whereas all three balance author's rights in his work versus third party's rights to copy, they represent different basic view points and legal framework, which directly affect the balancing point between the conflicting interests; The US default, as its name suggest – the "copy right", greatly differs from the European-civil law default, which stands for the "author's rights" in his work.
[111] Nissenbaum, footnote 3, at 797-803.
[112] O'Brien, David and Ullman, Jonathan and Altman, Micah and Gasser, Urs and Bar-Sinai, Michael and Nissim, Kobbi and Vadhan, Salil and Wojcik, Michael John and Wood, Alexandra, (2015) 'Integrating Approaches to Privacy Across the Research Lifecycle: When Is Information Purely Public?' Berkman Centre Research Publication No. 2015-7 [Discussing the management of confidential research data and the integration of methods to preserve confidentiality and secure privacy while promoting research in the Big Data era. Analysing privacy concerns through the lens of new sources of data and technological developments brought researchers to rethink boundaries between public and private and evoke the possible need for a new definition of "Public for Research Purposes."]

Scholars, Nissenbaum, Solove, and others' work reported above, highlight a similar rational in identifying the need for a revised paradigm that redefines governing dichotomies in which privacy may be maintained in light of competing interests as Open Justice.

Striking the right balance with tailor made solutions approach

Clearly, a categorical opposition to electronic access to court records is not an alternative. An overall rejection of digital access is not suggested even by those raising the most profound concerns on practices of online access. Similarly, overly broad access that reaches beyond the interests of the right to information, allowing for either the exploitation or manipulation of the data is a mechanism of potentially devastating results. It is broadly agreed upon that technological advancements in the digital age does not need to change the long-standing presumption of openness. Rather, now more than ever, this presumption is subjected to questions of degree, and the disclosure of judicial information should be limited at times.[113]

Striking the right balance, *conceptually*, is possible by adopting the contextual school of thought that rejects traditional dichotomies and acknowledges the changing nature of information (and privacy); when recognizing "that information in public records can still remain private even if there is limited access to it… a workable compromise for the tension between transparency and privacy emerges."[114] Static solutions that suited a world shaped by human restrictions such as cost and physical access,[115] led to the establishment of defaults. New technologies can provide tailor-made, scalable solutions, that answer the needs of various values, simultaneously. [116]

[113] Solove, n 1 [Broadly, in reconciling the tension between transparency and privacy, Solove contend that striking the proper balance between those competing interests is possible by limiting access or uses of certain information, rather than making public records unavailable]; Cohen, Julie E., Privacy, Visibility, Transparency, and Exposure. University of Chicago Law Review, Vol. 75, No. 1, 2008 [acknowledging that transparency and exposure, while being independent harms to privacy, should not be regulated against categorically but are subjected to "questions of degree".]

[114] Ibid, Solove.

[115] Nissenbaum, n 3, at 787 [Discussing traditional restrictions on access to court records. Whereas the theoretical framework of restricting right to access applies for digital access as well, some of the "physical world" restrictions are obviously less relevant or require some modification in order to fit the virtual arena. For an example, conditioning physical access to records at the Courthouse in an identification process seems to be a non-issue in the digital age, in which each device is constantly identified and monitored through a unique labelling known as Internet Protocol address (IP address).]

[116] For an example, a double copy system in which one complete version is kept discrete and a partially anonymized version is published. Anonymization is based on empirical findings and classifications of data categories, where sensitive data is defined differently in varies branches of law, and possibly even within different proceedings. Such

On the *pragmatic* level, an important practical question involves identifying and determining the dominant agents to regulate access. Unlike traditional-physical access determined mainly by judges, the practice of granting online access to court records includes a greater number of actors, from government agents (usually court administration) who initially publish the cases – to Internet intermediaries (i.e., third parties that provide infrastructure or platforms for accessing the information such as Internet Service Providers, search engines, and content providers). Considering each actor's rule in this information supply chain, and assuming clear legislative guidance, it seems that a government official in charge of the initial publication of the data is best situated to condition access to certain information, both normatively and practically. Not only is the government the first to release the data and is thus best positioned to control the subsequent information flow, but, once the information is publicly accessible, it would be both practically impossible and undesirable to limit access to it via the intermediaries. This is particularly true in light of the established rule that "once the government makes information public, the government cannot subsequently sanction its further disclosure."[117] This does not preclude additional layer of regulation imposed on intermediaries, for example, limiting subsequent exploitation of court records for commercial purposes.[118] Secondary to setting the legislative and policy framework to be issued by the agents in charge of publication, courts will maintain their traditional function in balancing competing interests on a case by case basis. Legal jurisdictions worldwide, particularly common law systems, are well acquainted with the delicate procedure of balancing competing interests. The task of balancing transparency and privacy interests should not be much different,[119] when weighing the benefits gained from disclosure versus the potential risk or harm caused by it, considering the various elements involved in

mechanism could be complemented with a list of permissible uses of court records. See two version solution as offered by Nissenbaum, n 3 And Gottlieb, n 60 discussing the concept of permissible uses defined by courts.

[117] Solove, n 1, at 1199-1202 [Referring to a line of cases in US courts held that it would be unlawful to prohibit a third party, in those cases mainstream media, from disclosing information that was truthful and lawfully obtained from public records.]

[118] Solove, n 1, 1189-1194 [On reconciling transparency and privacy by focusing on the purposes of granting access, limiting commercial uses for example, and curtailing personal information that does not promote the rational of allowing public scrutiny over government functioning.]; See also Gottlieb, n 60 [suggesting a list of "permissible uses"]; and also n 25 on the practice of charging individuals for data removal by content providers.

[119] Winn, n 8

electronic access to court records such as the type of information at hand, the practical ability to prevent disclosure, etc.[120]

When decision-makers consider legal and policy implementations, these are just some of the factors that need to be taken into account. The type of procedure (should a criminal process for example be more or less protected compared with a civil case? While the public has a greater interest in criminal proceedings, these presumably pose broader privacy exposure); Type of legal documents (this work related mostly to court decisions, yet the underlying questions should apply to other legal documents as well; Particularly, to legal document that contains sensitive data[121]; Date of legal proceeding (should current cases be distinguished from those that predated the internet due to higher level of privacy expectation in the pre-internet era?); The purpose of disclosure, type of database and the mechanism allowing access[122] (just middle ground policy recommendations suggests compiling a list of permissible uses and restricting access for purposes of commercial use)[123]; and most importantly, classification of information categories (taking into account re-identification technologies and what should count as personal/identifiable data[124]).

The widespread current practice of complete or partial anonymization should be broadly viewed as justified and therefore continued.[125] Limiting access to sensitive information in order to

[120] Note for example the balancing test provided by the U.S. Court of Appeals for the Third Circuit in the *Westinghouse* case, setting out five factors to be considered when balancing between privacy and governmental interest in disclosure of health records: (1) the type of health record in question and the type of health information it includes (2) the potential harm in non-disclosure of the information (3) the potential damage from disclosure (4) the ability to prevent unauthorized disclosure, and (5) the degree of need for access. *Westinghouse Electric Corp. v. United States* [1980] 638 F.2d 570 (3d Cir. 1980)

[121] Project by David Ardia and Anne Klinefelter on Privacy and Court Records shows for example that whereas intuition leads to the belief that sensitive data appears in appendixes more than in briefs, it is in fact the other way around, see project preliminary findings as presented in UC Berkeley Law Conference on Open Government Data (2015) < https://www.law.berkeley.edu/files/David_Ardia_Privacy_and_Court_Records_BCLT_Presentation.pdf > accessed 25 April 2016

[122] See discussion in part I to this paper and reference there to differentiating between profit and non-profit databases.

[123] n 118.

[124] An analogous can be seen in a question debated by most European countries on whether IP address count as identifiable data given the technical ability to link between each address and an individual.

[125] Nissenbaum, footnote 3, at 825 [discussing inter alia, the justification of preventing stigma or shame, as well as preventing harm to one of the litigating parties or a third party] and also in 839-341 [Arguing that sanitizing court records by redacting names and identification data will "lowers the stakes of providing free and unrestricted online access and diminishes pressure to seal or redact other information typically deemed sensitive".]

protect privacy is an established principle.[126] Sanitizing court records prior to their publication embodies some technical and normative difficulties: is anonymization feasible or effective?[127] Are individuals in a society willing to compromise the "important dimension of answerability from the courts, for example, assurances that there is no discrimination for or against plaintiffs or defendants based on race, ethnicity, economic standing, or other inappropriate dimensions?"[128]

As a matter of principle, sensitive information is not likely to promote openness and thus, considering the underlying rational of granting access (as transparency, fairness, accountability and public scrutiny), information categories that do not contribute to it should be omitted from the records. A key element that differentiates one sanitization method from another, concerns the importance of exposing parties' names when balancing openness and privacy interests. On the one hand, indeed there seems to be a "plethora of facts far more relevant to the public than the litigants' names"[129]. Generally, parties to a legal case (particularly Plaintiffs in civil cases and Defendants, especially those wrongfully accused) would prefer pseudonym status to avoid signalling litigiousness and any potential harm to reputation.[130] One the other hand, as stated above, knowledge should supersede ignorance;[131] some studies indicate that it is prissily the

[126] Nissenbaum, n 5, at 128-129 [referring to specific categories of sensitive information including medical information, certain financial information etc.]

[127] A respected body of literature holds the assumption that in a "Big Data" era, where databases may be cross-reference and with technologies of re-identification, anonymization no longer poses a viable solution. For reading on the growing lack of confidence in anonymization See A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In S&P, 2008; Narayanan, A. and Shmatikov, V. Myths and fallacies of 'personally identifiable information.' (2010) Commun. ACM 53, 6; Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA L. REV. 1701, 2010.

[128] Nissenbaum, footnote 3, at 841-842 [stating that sanitizing courts records will not allow monitoring instances when harsher sentences are given to defendants of a particular race for example]; A MacArthur genius winning research, 'looking death worthy' by Eberhardt et al. that showed the impact of stereotypical perception of Blacks on death sentences is arguably impossible to conduct in Spain or France, where decisions are anonymized. Eberhardt, Jennifer L.; Davies, P G.; Purdie-Vaughns, Valerie J.; and Johnson, Sheri Lynn, 2006. 'Looking Deathworthy: Perceived Stereotypicality of Black Defendants Predicts Capital-Sentencing Outcomes' (2006) Psychol Sci 17(5), 383.

[129] Lior Strahilevitz, 'Pseudonymous Litigation' (2010) 77 U. CHI. L. REV. 1239, 1246; Caren Myers Morrison, 'Privacy, Accountability and the Cooperating Defendant: Towards a New Role for Internet Access to Court Records' (2009) 62 VAND. L. REV. 921, 971 [Arguing that their party's names should be omitted based as they do not contribute to the principle of openness].

[130] Ibid, Strahilevitz [Examining informal process in the form of feedback sites as a viable alternative to formal adjudication in certain instances, suggesting (1) that some controversies should be steered out of courts (2) Given that pseudonymous complaints have become increasingly available in the Information Age (via feedback sites), pseudonymity may be used in formal litigation as a device to sort grievances between informal and formal dispute resolution mechanisms; further theorizing the "prevailing party pseudonymity" rule as an ex ante shortcut for sorting grievances, according to which only the litigant who ultimately loses is named.]

[131] See chapter on Economic Theory of privacy and references there to Posner (n 47) and Strahilevitz (n 50)

exposure of name that may eventually benefit the involved parties. Furthermore, from a public interest' perspective, the importance of being able to tie a certain name to a particular injurer cannot be overstated[132] and is an inherent part of the judicial process, particularly with regard to criminal justice.

Conclusion

Further research is needed in determining the proper legislative and policy framework to define electronic access to court records. In line of the above stated, it is clear that no categorical answer should be used in the dialogue on privacy *and* publicity when considering digital open doors to court houses. The French approach aforementioned defines the Internet as a "revolution". Whether or not the Internet has changed everything is too early to tell. The diametric approach, according to which the presumption in favour of public access to court records should not shift depending on the medium, is also questionable. Without a doubt, the Internet has changed *something*. A thorough thinking that acknowledges this change while respecting long-lasting legal traditions, is a good place to start thinking about the matter of online access to court records.

[132] Strahilevitz, n 129, at 1257-1258 [Discussing the ability to identify a specific injurer as one critical advantage of formal litigation over online dispute sites, which usually facilitates anonymous and pseudonymous speech.]