INTRODUCTION

Habeas Data is a latin word which can be loosely translated to mean “have the data”. The right has been primarily conceptualized, designed, ratified, and implemented by various nation-states in the background of a shared common history of decades of torture, terror, and other repressive practices under military juntas and other fascist regimes. The writ of *habeas data* was a distinct response to these recent histories which provided individuals with basic rights to access personal information collected by the state (and sometimes byprivate agencies of a public nature) and to challenge and correct such data, requiring the state to safeguard the privacy and accuracy of people's personal data.[1]

The origins of Habeas Data are traced back, unsurprisingly, to the European legal regime since Europe is considered as the fountainhead of modern data protection laws. The inspiration for Habeas Data is often considered to be the Council of Europe's 108th Convention on Data Protection of 1981.[2] The purpose of the Convention was to secure the privacy of individuals regarding the automated processing of personal data. For this purpose, individuals were granted several rights including a right to access their personal data held in an automated database.[3]

Another source or inspiration behind Habeas Data is considered to be the German legal system where a constitutional right to information self-determination was created by the German Constitutional Tribunal by interpretation of the existing rights of human dignity and personality. This is a right to know what type of data is stored on manual and automatic databases about an individual, and it implies that there must be transparency on the gathering and processing of such data.[4]

Habeas Data is essentially a right or mechanism for an individual complaint presented to a constitutional court, to protect the image, privacy, honour, information self-determination and freedom of information of a person.[5] A Habeas Data complaint can be filed by any citizen against any register to find out what information is held about his or her person. That person can request the rectification, update or even the destruction of the personal data held, it does not matter most of the times if the register is private or public.[6]

---

1 González, Marc-Tizoc, ‘Habeas Data: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance’, (2015). Chicago-Kent Law Review, Vol. 90, No. 2, 2015; St. Thomas University School of Law (Florida) Research Paper No. 2015-06. Available at SSRN:http://ssrn.com/abstract=2694803

2 Article 8 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

3 Guadamuz A, 'Habeas Data: The Latin-American Response to Data Protection',2000 (2) *The Journal of Information, Law and Technology (JILT)*.

4 *Id.*

5 Speech by Chief Justice Reynato Puno, Supreme Court of Philippines delivered at the *UNESCO Policy Forum and Organizational Meeting of the Information for all Program (IFAP), Philippine National Committee*, on November 19, 2007, available at http://jlp-law.com/blog/writ-of-habeas-data-by-chief-justice-reynato-puno/

6 Guadamuz A, 'Habeas Data: The Latin-American Response to Data Protection',2000 (2) *The Journal of Information, Law and Technology (JILT)*.

Habeas Data in different jurisdictions

Habeas Data does not have any one specific definition and has different characteristics in different jurisdictions. Therefore, in order to better understand the right, it will be useful to describe the scope of Habeas Data as it has been incorporated in certain jurisdictions in order to better understand what the right entails:[7]

Brazil

The Constitution of Brazil grants its citizens the right to get a habeas data "a. to assure knowledge of personal information about the petitioner contained in records or data banks of government agencies or entities of a public character; b. to correct data whenever the petitioner prefers not to do so through confidential judicial or administrative proceedings;"[8] The place or tribunal where the Habeas Data action is to be filed changes depending on who is it presented against, which creates a complicated system of venues. Both the Brazilian constitution and the 1997 law stipulate that the court will be:

- The Superior Federal Tribunal for actions against the President, both chambers of Congress and itself;
- The Superior Justice Tribunal for actions against Ministers or itself;
- The regional federal judges for actions against federal authorities;
- State tribunals according to each state law;
- State judges for all other cases.[9]

Paraguay

The Constitution of Paraguay grants a similar right of habeas data in its constitution which states:

"All persons may access the information and the data that about themselves, or about their assets, [that] is [obren] in official or private registries of a public character, as well as to know the use made of the same and of their end. [All persons] may request before the competent magistrate the updating, the rectification or the destruction of these, if they were wrong or illegitimately affected their rights."[10]

---

[7] The author does not purport to be an expert on the laws of these jurisdictions and the analysis in this paper has been based on a reading of the actual text or interpretations given in the papers that have been cited as the sources. The views in this paper should be viewed keeping this context in mind.

[8] Article 5, LXXII of the Constitution of Brazil, available at https://www.constituteproject.org/constitution/Brazil_2014.pdf

[9] Guadamuz A, 'Habeas Data vs the European Data Protection Directive', Refereed article, 2001 (3) *The Journal of Information, Law and Technology (JILT)*.

[10] Article 135 of the Constitution of Paraguay, available at https://www.constituteproject.org/constitution/Paraguay_2011.pdf?lang=en

Compared to the right granted in Brazil, the text of the Paraguay Constitution specifically recognises that the citizen also has the right to know the use his/her data is being put to.

Argentina

Article 43 of the Constitution of Argentina grants the right of habeas data, though it has been included under the action of "amparo"[11], the relevant portion of Article 43 states as follows:

"Any person may file an amparo action to find out and to learn the purpose of data about him which is on record in public registries or data banks, or in any private [registers or data banks] whose purpose is to provide information, and in case of falsity or discrimination, to demand the suppression, rectification, confidentiality, or updating of the same. The secrecy of journalistic information sources shall not be affected."[12]

The version of Habeas Data recognised in Argentina includes most of the protections seen in Brazil and Paraguay, such as the right to access the data, rectify it, update it or destroy it, etc. Nevertheless, the Argentinean constitution also includes certain other features such as the fact that it incorporates the Peruvian idea of confidentiality of data, being interpreted as the prohibition to broadcast or transmit incorrect or false information. Another feature of the Argentinean law is that it specifically excludes the press from the action, which may be considered as reasonable or unreasonable depending upon the context and country in which it is applied.[13]

Venezuela

Article 28 of the Constitution of Venezuela established the writ of *habeas data*, which expressly permits access to information stored in official and private registries. It states as follows:

"All individuals have a right to access information and data about themselves and about their property stored in official as well as private registries. Secondly, they are entitled to know the purpose of and the policy behind these registries. Thirdly, they have a right to request, before a competent tribunal, the updating, rectification, or destruction of any database that is inaccurate or that undermines their entitlements. The law shall establish exceptions to these principles. By the same token, any person shall have access to information that is of interest to communities and groups. The secrecy of the sources of newspapers-and of other entities or individuals as defined by law-shall be preserved."[14]

---

[11] The petition for a writ of amparo is a remedy available to any person whose right to life, liberty and security is violated or threatened with violation by an unlawful act or omission of a public official or employee, or of a private individual or entity.

[12] Article 43 of the Constitution of Argentina, available at https://www.constituteproject.org/constitution/Argentina_1994.pdf?lang=en

[13] https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz/

[14] Article 28 of the Venezuelan Constitution, available at http://www.venezuelaemb.or.kr/english/ConstitutionoftheBolivarianingles.pdf

The Venezuelan writ of *habeas data* expressly provides that individuals "are entitled to know the purpose of and the policy behind these registries." Also, it expresses a right to "updating, rectification, or destruction of any database that is inaccurate or that undermines their entitlements." Article 28 also declares that the "secrecy of the sources of newspapers and of other entities or individuals as defined by law-shall be preserved."[15]

Philippines

It is not as if the remedy of Habeas Data is available only in Latin American jurisdictions, but even in Asia the writ of Habeas Data has been specifically granted by the Supreme Court of the Philippines vide its resolution dated January 22, 2008 which provides that "The writ of habeas data is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party." According to the Rule on Writ of Habeas Data, the petition is to be filed with the Regional Trial Court where the petitioner or respondent resides, or which has jurisdiction over the place where the data or information is gathered, collected or stored, at the option of the petitioner. The petition may also be filed with the Supreme Court or the Court of Appeals or the Sandiganbayan when the action concerns public data files of government offices.[16]

Two major distinctions are immediately visible between the Philippine right and that in the latin jurisdictions discussed above. One is the fact that in countries such as Bazil, Argentina and Paraguay, there does not appear to be a prerequisite to filing such an action asking for the information, whereas in Philippines it seems that such a petition can only be filed only if an individual's "right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission". This means that the Philippine concept of habeas data is much more limited in its scope and is available to the citizens only under certain specific conditions. On the other hand the scope of the Philippine right of Habeas Data is much wider in its applicability in the sense that this right is available even against private individual and entities who are "engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence". In the Latin American jurisdictions discussed above, this writ appears to be available only against either public institutions or private institutions having some public character.

Main features of Habeas Data

---

[15] González, Marc-Tizoc, 'Habeas Data: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance', (2015). Chicago-Kent Law Review, Vol. 90, No. 2, 2015; St. Thomas University School of Law (Florida) Research Paper No. 2015-06. Available at SSRN:http://ssrn.com/abstract=2694803

[16] Rule on the Writ of Habeas Data Resolution, available at http://hrlibrary.umn.edu/research/Philippines/Rule%20on%20Habeas%20Data.pdf

Thus from the discussion above, the main features of the writ of habeas data, as it is applied in various jurisdictions can be culled out as follows:[17]

- It is a right to the individual or citizen to ask for his/her information contained with any data registry;
- It is available only against public (government) entities or employees; or private entities having a public character;[18]
- Usually it also gives the individuals the right to correct any wrong information contained in the data registry;
- It is a remedy that is usually available by approaching any single judicial forum.

Since the writ of Habeas Data has been established and evolved primarily in Latin American countries, there is not too much literature on it available freely in the English language and that is a serious hurdle in researching this area. For example, this author did not find many article mentioning the scope of the writ of habeas data, for example whether it is an absolute right and on what grounds can it be denied. The Constitution of Venezuela, for example, specifies that the law shall establish exceptions to these principles and infact mentions the secrecy of sources for newspapers as an exception to this rule.[19] Similarly in Argentina, there exists a public interest exception to the issuance of the writ of Habeas Data.[20] That said, although little literature on the specific exceptions to habeas data is freely available in English, references can still be found to exceptions such as state security (Brazil), secrecy of newspaper sources (Argentina and Venezuela), or other entities defined by law (Venezuela).[21] This suggests that the, as would be expected, the right to ask for the writ of habeas data is not an absolute right but would also be subject to certain exceptions and balanced against other needs such as state security and police investigations.

Habeas Data in the context of Privacy

---

[17] The characteristics of habeas data culled out in this paper are by no means exhaustive and based only on the analysis of the jurisdictions discussed in this paper. This author does not claim to have done an exhaustive analysis of every jurisdiction where Habeas Data is available and the views in this paper should be viewed in that context.

[18] Except in the case of the Philippines and Venezeula. This paper has not done an analysis of the writ of habeas data in every jurisdiction where it is available and there may be jurisdictions other than the Philippines which also give this right against private entities.

[19] González, Marc-Tizoc, 'Habeas Data: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance', (2015). Chicago-Kent Law Review, Vol. 90, No. 2, 2015; St. Thomas University School of Law (Florida) Research Paper No. 2015-06. Available at SSRN:http://ssrn.com/abstract=2694803

[20] The case of *Ganora v. Estado Nacional*, Supreme Court of Argentina, September 16, 1999, *cf.*http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Argentin.html

[21] González, Marc-Tizoc, 'Habeas Data: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance', (2015). Chicago-Kent Law Review, Vol. 90, No. 2, 2015; St. Thomas University School of Law (Florida) Research Paper No. 2015-06. Available at SSRN:http://ssrn.com/abstract=2694803

Data protection legislation and mechanisms protect people against misuse of personal information by data controllers. **Habeas Data**, being a figure for use only by certain countries, gives the individuals the right to access, correct, and object to the processing of their information.

In general, privacy is the genus and data protection is the species, data protection is a right to personal privacy that people have against the possible use of their personal data by data controllers in an unauthorized manner or against the requirements of force. Habeas Data is an action that is brought before the courts to allow the protection of the individual's image, privacy, honour, self-determination of information and freedom of information of a person. In that sense, the right of Habeas Data can be found within the broader ambit of data protection. It does not require data processors to ensure the protection of personal data processed but is a legal action requiring the person aggrieved, after filing a complaint with the courts of justice, the access and/or rectification to any personal data which may jeopardize their right to privacy.[22]

Habeas Data in the Indian Context

Although a number of judgments of the Apex Court in India have recognised the existence of a right to privacy by interpreting the fundamental rights to life and free movement in the Constitution of India,[23] the writ of habeas data has no legal recognition under Indian law. However, as is evident from the discussion above, a writ of habeas data is very useful in protecting the right to privacy of individuals and it would be a very useful tool to have in the hands of the citizens. The fact that India has a fairly robust right to information legislation means that atleast some facets of the right of habeas data are available under Indian law. We shall now examine the Indian Right to Information Act, 2005 (RTI Act) to see what facets of habeas data are already available under this Act and what aspects are left wanting.

As mentioned above, the writ of habeas data has the following main features:

- It is a right to the individual or citizen to ask for his/her information contained with any data registry;
- It is available only against public (government) entities or employees; or private entities having a public character;[24]
- Usually it also gives the individuals the right to correct any wrong information contained in the data registry;
- It is a remedy that is usually available by approaching any single judicial forum.

---

[22] http://www.oas.org/dil/data_protection_privacy_habeas_data.htm

[23] Even the scope of the right to privacy is currently under review in the Supreme Court of India. See "Right to Privacy in Peril", http://cis-india.org/internet-governance/blog/right-to-privacy-in-peril

[24] Except in the case of the Philippines. This paper has not done an analysis of the writ of habeas data in every jurisdiction where it is available and there may be jurisdictions other than the Philippines which also give this right against private entities.

We shall now take each of these features and analyse whether the RTI Act provides any similar rights and how they differ from each other.

Right to seek his/her information contained with a data registry

Habeas data enables the individual to seek his or her information contained in any data registry. The RTI Act allows citizens to seek "information" which is under the control of or held by any public authority. The term information has been defined under the RTI Act to mean "any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force".[25] Further, the term "record" has been defined to include "(a) any document, manuscript and file; (b) any microfilm, microfiche and facsimile copy of a document; (c) any reproduction of image or images embodied in such microfilm (whether enlarged or not); and (d) any other material produced by a computer or any other device". It is quite apparent that the meaning given to the term information is quite wide and can include various types of information within its fold. The term "information" as defined in the RTI Act has been further elaborated by the Supreme Court in the case of *Central Board of Secondary Education* v. *Aditya Bandopadhyay*,[26] where the Court has held that a person's evaluated answer sheet for the board exams held by the CBSE would come under the ambit of "information" and should be accessible to the person under the RTI Act.[27]

An illustrative list of items that have been considered to be "information" under the RTI Act would be helpful in further understanding the concept:

(i) Asset declarations by Judges;[28]

(ii) Copy of inspection report prepared by the Reserve Bank of India about a Co-operative Bank;[29]

(iii) Information on the status of an enquiry;[30]

---

25 Section 2(f) of the Right to Information Act, 2005.

26 2011 (106) AIC 187 (SC), also available at http://judis.nic.in/supremecourt/imgst.aspx?filename=38344

27 The exact words of the Court were: "The definition of `information' in section 2(f) of the RTI Act refers to any material in any form which includes records, documents, opinions, papers among several other enumerated items. The term `record' is defined in section 2(i) of the said Act as including any document, manuscript or file among others. When a candidate participates in an examination and writes his answers in an answer-book and submits it to the examining body for evaluation and declaration of the result, the answer-book is a document or record. When the answer-book is evaluated by an examiner appointed by the examining body, the evaluated answer-book becomes a record containing the `opinion' of the examiner. Therefore the evaluated answer-book is also an `information' under the RTI Act."

28 *Secretary General, Supreme Court of India* v. *Subhash Chandra Agarwal*, AIR 2010 Del 159, available at https://indiankanoon.org/doc/1342199/

29 *Ravi Ronchodlal Patel* v. *Reserve Bank of India*, Central Information Commission, dated 6-9-2006.

30 *Anurag Mittal* v. *National Institute of Health and Family Welfare*, Central Information Commission, dated 29-6-2006.

(iv) Information regarding cancellation of an appointment letter;[31]

(v) Information regarding transfer of services;[32]

(vi) Information regarding donations given by the President of India out of public funds.[33]

The above list would indicate that any personal information relation to an individual that is available in a government registry would in all likelihood be considered as "information" under the RTI Act.

However, just because the information asked for is considered to come within the ambit of section 2(h) does not mean that the person will be granted access to such information if it falls under any of the exceptions listed in section 8 of the RTI Act. Section 8 provides that if the information asked falls into any of the categories specified below then such information shall not be released in an application under the RTI Act, the categories are:

"(a) information, disclosure of which **would prejudicially affect the sovereignty and integrity of India,** the security, strategic, scientific or economic interests of the State, relation with foreign State or lead to incitement of an offence;

(b) information which has been expressly **forbidden to be published by any court** of law or tribunal or the disclosure of which may constitute contempt of court;

(c) information, the disclosure of which would **cause a breach of privilege of Parliament** or the State Legislature;

(d) information including **commercial confidence, trade secrets or intellectual property,** the disclosure of which would harm the competitive position of a third party, unless the competent authority is satisfied that larger public interest warrants the disclosure of such information;

(e) information **available to a person in his fiduciary relationship**, unless the competent authority is satisfied that the larger public interest warrants the disclosure of such information;

(f) information **received in confidence from foreign Government**;

(g) information, the **disclosure of which would endanger the life or physical safety of any person** or identify the source of information or assistance given in confidence for law enforcement or security purposes;

(h) information which would **impede the process of investigation** or apprehension or prosecution of offenders;

(i) **cabinet papers** including records of deliberations of the Council of Ministers, Secretaries and other officers:

---

31 *Sandeep Bansal* v. *Army Headquarters, Ministry of Defence*, Central Information Commission, dated 10-11-2008.

32 *M.M. Kalra* v. *DDA*, Central Information Commission, dated 20-11-2008.

33 *Nitesh Kumar Tripathi* v. *CPIO*, Central Information Commission, dated 4-5-2012.

Provided that the decisions of Council of Ministers, the reasons thereof, and the material on the basis of which the decisions were taken shall be made public after the decision has been taken, and the matter is complete, or over:

Provided further that those matters which come under the exemptions specified in this section shall not be disclosed;

(j) **information which relates to personal information** the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information:

Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person."

The abovementioned exceptions seem fairly reasonable and infact are important since public records may contain information of a private nature which the data subject would not want revealed, and that is exactly why personal information is a specific exception mentioned under the RTI Act. When comparing this list to the recognised exceptions under habeas data, it must be remembered that a number of the exceptions listed above would not be relevant in a habeas data petition such as commercial secrets, personal information, etc. The exceptions which could be relevant for both the RTI Act as well as a habeas data writ would be (a) national security or sovereignty, (b) prohibition on publication by a court, (c) endangering the physical safety of a person, (d) hindrance in investigation of a crime. It is difficult to imagine a court (especially in India) granting a habeas data writ in violation of these four exceptions.

Certain other exceptions that may be relevant in a habeas data context but are not mentioned in the common list above are (a) information received in a fiduciary relationship; (b) breach of legislative privilege, (c) cabinet papers; and (d) information received in confidence from a foreign government. These four exceptions are not as immediately appealing as the others listed above because there are obviously competing interests involved here and different jurisdictions may take different points of view on these competing interests.[34]

Available only against public (government) entities or entities having public character

A habeas corpus writ is maintainable in a court to ask for information relating to the petitioner held by either a public entity or a private entity having a public character. In India, the right to information as defined in the RTI Act means the right to information accessible under the Act held by or under the control of any public authority. The term "public authority" has been defined under the Act to mean "any authority or body or institution of self-government established or constituted—

(a) by or under the Constitution;

[34] A similar logic may apply to the exceptions of (i) cabinet papers, and (ii) parliamentary privilege.

(b) by any other law made by Parliament;

(c) by any other law made by State Legislature;

(d) by notification issued or order made by the appropriate Government, and includes any—(i) body owned, controlled or substantially financed; (ii) non-Government organisation substantially financed, directly or indirectly by funds provided by the appropriate Government;"[35]

Therefore most government departments as well as statutory as well as government controlled corporations would come under the purview of the term "public authority". For the purposes of the RTI Act, either control or substantial financing by the government would be enough to bring an entity under the definition of public authority.[36] The above interpretation is further bolstered by the fact that the preamble of the RTI Act contains the term "governments and their instrumentalities".[37]

Right to correct wrong information

While certain sectoral legislations such as the Representation of the People Act and the Collection of Statistics Act, etc. may provide for correction of inaccurate information, the RTI Act does not have any such provisions. This stands to reason because the RTI Act is not geared towards providing people with information about themselves but is instead a transparency law which is geared at dissemination of information, which may or may not relate to an individual.

Available upon approaching a single judicial forum

While the right of habeas data is available only upon approaching a judicial forum, the right to information under the RTI Act is realised entirely through the bureaucratic machinery. This also means that the individuals have to approach different entities in order to get the information that they need instead of approaching just one centralised entity.

---

35 Section 2 (h) of the Right to Information Act, 2005.

36 *M.P. Verghese* v. *Mahatma Gandhi University*, 2007 (58) AIC 663 (Ker), available at https://indiankanoon.org/doc/1189278/

37 *Principal, M.D. Sanatan Dharam Girls College, Ambala City* v. *State Information Commissioner*, AIR 2008 P&H 101, available at https://indiankanoon.org/doc/1672120/

Conclusion

There is no doubt that *habeas data*, by itself cannot end massive electronic surveillance of the kind that is being carried out by various governments in this day and age and the excessive collection of data by private sector companies, but providing the citizenry with the right to ask for such a writ would provide a critical check on such policies and practices of vast surveillance.[38] An informed citizenry, armed with a right such as *habeas data*, would be better able to learn about the information being collected and kept on them under the garb of law and governance, to access such information, and to demand its correction or deletion when its retention by the government is not justified.

As we have discussed in this paper, under Indian law the RTI Act gives the citizens certain aspects of this right but with a few notable exceptions. Therefore, if a writ such as habeas data is to be effectuated in India, it might perhaps be a better idea to approach it by amending/tweaking the existing structure of the RTI Act to grant individuals the right to correct mistakes in the data along with creating a separate department/mechanism so that the applications demanding access to one's own data do not have to be submitted in different departments but can be submitted at one central place. This approach may be more pragmatic rather than asking for a change in the Constitution to grant to the citizens the right to ask for a writ in the nature of habeas data.

There may be calls to also include private data processors within the ambit of the right to habeas data, but it could be challenging to enforce this right. This is because it is still feasible to assume that the government can put in place machinery to ensure that it can find out whether information about a particular individual is available with any of the government's myriad departments and corporations, however it would be almost impossible for the government to track every single private database and then scan those databases to find out how many of them contain information about any specific individual. This also throws up the question whether a right such as habeas data, which originated in a specific context of government surveillance, is appropriate to protect the privacy of individuals in the private sector. Since under Indian law section 43A and the Rules thereunder, which regulate data protection, already provide for consent and notice as major bulwarks against unauthorised data collection, and limit the purpose for which such data can be utilised, privacy concerns in this context can perhaps be better addressed by strengthening these provisions rather than trying to extend the concept of habeas data to the private sector.

---

[38] González, Marc-Tizoc, 'Habeas Data: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance', (2015). Chicago-Kent Law Review, Vol. 90, No. 2, 2015; St. Thomas University School of Law (Florida) Research Paper No. 2015-06. Available at SSRN:http://ssrn.com/abstract=2694803