INFORMATION LAW JOURNAL

A Publication of the Information Security & Internet of Things Committees
ABA Section of Science & Technology Law

SUMMER 2019 VOLUME 10 ISSUE 3 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

An Algorithmic Approach for Choice-of-Law

By Elizabeth Davidson

How does the mechanism of law work? What does it *do*? Is it "a standard procedure that involves a number of steps, which if followed correctly, can be relied upon to lead to the solution of a particular kind of problem"?[1] Or does it work like a "finite set of unambiguous instructions that, given some set of initial conditions, *Read more*

The Next Big One for the Software Industry. Is Your ePrivacy Preparedness Kit Ready?

By Volha Samasiuk and Alex Gin

As we mark the one-year anniversary of the General Data Protection Regulation (the "GDPR") coming into effect, major enforcement cases with multi-million dollar fines have been largely absent. But as Helen Dixon recently noted, these cases are "not overnight." Many investigations are still in progress, and large *Read more*

An Analysis of the Legal Framework of e-Commerce in India

By Arunabh Choudhary and Tanvi Muraleedharan

In the last decade, India underwent a digitization revolution, there was a phenomenal shift that was felt in the market as India went online. According to Morgan Stanley the growth is driven by a combination of rising internet penetration, with high digital literacy in India and drop in data access costs and flow of *Read more*

Overview: Brazil's New Data Privacy Law

By Renato Opice Blum and Camila Rioja Arantes

The Brazilian House of Representatives approved the Brazilian data protection draft bill (PL 53/2018, "LGPD") on May 29, 2018. Following subsequent passage by the Federal Senate, the LGPD was signed into law by former President Temer on August 14, 2018[1]. On December 27, 2018, the Provisional Measure *Read more*

Another Depressing Day for U.S. Data Privacy

By Thomas Shaw

At one time, the United States was the leader in both data privacy legislation and enforcement. Unfortunately, those days are long since passed, seen clearly through the lack of a national data privacy statute that allows data subjects to always remain in control of their personal data and penalizes organizations that *Read more*

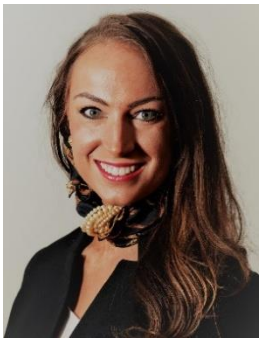
****Editor's Message****

We are into the tenth full year of publishing the *Information Law Journal* each quarter, continuing to welcome authors and readers from across the ABA. This issue again presents articles focusing on various aspects of leading-edge domestic and international practice in information, Internet, and emerging technologies law. Upward of 300 authors have written for the *Information Law Journal* and antecedents. Three authors are writing here for the first time.

Our next issue (Autumn 2019) is scheduled to be published in September 2019. All readers of the *Information Law Journal* may share their experiences and knowledge with their fellow professionals by writing an article. Every qualified submission within the scope and requirements as explained in the **Author Guidelines** will be published. The issue following the next issue (Winter 2020) is scheduled to be published in December 2019.

An Algorithmic Approach for Choice-of-Law

By Elizabeth Davidson



How does the mechanism of law work? What does it do? Is it "a standard procedure that involves a number of steps, which if followed correctly, can be relied upon to lead to the solution of a particular kind of problem"?[1] *Or does it work like a "finite set of unambiguous instructions that, given some set of initial conditions,* can be performed in a prescribed sequence to achieve a certain goal [with] a recognizable set of end conditions;"[2] does it carry out "a sequence of steps set out with the aim of solving a problem…a way of addressing questions sharing a similar character in a systematic manner"[3]? These definitions are instead permutations of the term "algorithm." Though, in reviewing these statements, it is hard to deny that *law*, in its essence of what we think of it to be, does not also match these definitions.[4] Instead of using democratic mechanisms to oversee the structure of computer technology as suggested by Lawrence Lessig,[5] the law may instead use technology to better effectuate its ends.[6]

As early as 1908, legal scholars such as Rosco Pound not only had reactions to legal formalism,[7] but also to the technical application of law as a science.[8] Exacting methods sometimes lead to results that are unfair, so legal realists refuted "artificiality in law as an end" but instead are driven to examine "the result to which [it] lead[s]."[9] At that time, an adherence to human's "love of technicality as a manifestation of cleverness," was a superficial response to "magisterial caprice"[10]—Pound's word for judicial discretion.[11] Pound acknowledged the problem of inconsistences in the law were pride in a

---

[1] Derek Haylock & Fiona Thangata, "Algorithm" KEY CONCEPTS IN TEACHING PRIMARY MATHEMATICS (2007) http://proxy.lib.uiowa.edu/login?url=https://search.credoreference.com/content/entry/sageuktpm/algorithm/0?institutionId=1049.

[2] "algorithm" THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (2016) http://proxy.lib.uiowa.edu/login?url=https://search.credoreference.com/content/entry/hmdictenglang/algorithm/0?institutionId=1049.

[3] "Algorithm" http://en.citizendium.org/wiki/Algorithm (last visited April 2, 2019).

[4] Paul Gowder, *Is Legal Cognition Computational? (When Will DeepVehicle Replace Judge Hercules?)* (2019) https://osf.io/preprints/lawarxiv/gk2ms. The Oxford Dictionary of Law defines law as "the enforceable body of rules that govern any society." *Law*, A DICTIONARY OF LAW. OXFORD UNIVERSITY PRESS, http://www.oxfordreference.com.proxy.lib.uiowa.edu/view/10.1093/acref/9780198802525.001.0001/acref-9780198802525-e-2186 (2018).

[5] *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[6] See Mireille Hildebrandt, *Saved by Design? The Case of Legal Protection by Design*, 307, 308 (Dec. 14, 2016) (indicating that awareness of the disrupting technology is not the end in law, but it is that protection of fundamental rights).

[7] William L. Grossman, *The Legal Philosophy of Roscoe Pound*, 44 YALE L.J. 605, 618 (1935) https://digitalcommons.law.yale.edu/ylj/vol44/iss4/2.

[8] *See generally* Roscoe Pound, *Mechanical Jurisprudence*, 8:8 COLUMBIA L. REV. (1908), 605-623.

[9] Roscoe Pound, *Mechanical Jurisprudence*, 8: 8 COLUMBIA L. REV. (1908), 605.

[10] *Id*.

[11] Later Larry Kramer proposed a "serious effort to harness judicial discretion in choice-of-law by setting forth rules for decision in common situations." William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 273 (2002).

strong decision by judges was one that "opposed common-sense and common convenience."[12] Yet the dichotomy between formalism and realism need not be mediated with modern algorithmic technology. Rather, technology has the capability to transcend it.[13] This paper seeks to shed light on the value of using such technology to avoid the problem formalists see, judicial exuberance, while also honoring the goals of legal realists, who maintain a pragmatic objective. Using the context of Conflicts of Law, I specifically seek to demonstrate the benefit of such technology to direct judges' temptation to use escape devices and instead to systematically apply the procedure and values posed by each forum state.

While the "thinking machines," were only coming into focus during the same time of these legal theories, it was unimaginable for 20th century legal scholars to develop a robust value-honoring choice-of-law system based on computers' capabilities. Both choice-of-law decisions and computer algorithms each work with a given set of parameters, the legal and factual inputs. And algorithms always work, which means that the program may take into account a wide variety of qualitative societal realities and can also do so in an accurate and systematic manner. Therefore, legal precedent and dynamic parameters of facts will work as the algorithm's inputs.[14] Thus, an algorithmic solution to the choice-of-law judicial reasoning is a way to honor legal integrity. Where "judges have never had time to take the trouble to analyze very clearly just what they do mean," a technological tool should be added to eliminate some of the busy work and better refine the scope of judges' possible decisions.[15]

Therefore, this paper will first show a classic instance of the problem regarding ambiguity in law. In applying an algorithmic approach to a basic misdemeanor problem, this part warms up the reader for a more complicated algorithmic application for choice-of-law. The next section of this paper will show the level of ambiguity in the conflicts space and describe some valiant attempts from scholars and legal drafters to provide more clarity. In bringing out and describing the judicial reasoning problem in Conflicts, the theoretical and pragmatic reasons for a change will be discussed. Finally, an example of how the algorithmic approach would work through the lens seminal conflict of law case, *Millikin*, is discussed below.[16] Limitations and suggestions for an algorithmic solution introduced into the American legal system will also be discussed.[17]

This paper contains a few assumptions. The first assumption is that clarity and precision law is desired. A judicial "caprice" is not an epistemologically healthy way for law to function. While "[e]veryone

---

[12] Roscoe Pound, *Mechanical Jurisprudence*, 8:8 COLUMBIA L. REV. 605, 608 (1908) (quoting Chief Justice Erle).
[13] The simple fact that the algorithms are not programmed into computer software does not mean that the mechanisms of law are not an algorithmic. Transcending this dichotomy is not a new idea. *See* IAN AYRES & JOHN BRAITHWAITE. RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE (1992).
[14] See *Infra* Part IV.C.
[15] Walter W. Cook, *The Logical and Legal Basis of the Conflict of Law*, 33 YALE L.J. 484 (1924).
[16] *Infra* Part II.C.
[17] *Infra* Parts IV & V.

scorns judicial activism, that notoriously slippery term,"'[18] the ideal legal system contains a judge's tough decisions to be made closer to the mechanics of a computer than politician. Even if the reader allows a judge to act as policymaker,[19] the reader undoubtedly accepts the premise of federalism, full faith and credit, and sovereignty of each state to make and enforce their own laws.[20] Conflicts is therefore a place that an algorithmic approach to law not only could be helpful but provides the best approach to the choice-of-law problems because the complexities compounded with constitutional parameters. Finally, this article presumes that an algorithmic approach to Conflicts has not been explored. Although the technology is available to apply such an approach, it is clear a theoretical basis from which to explore technological application could be helpful in this area of law.[21]

I. Traditional Legal Ambiguity

First, a classic instance of the problem regarding ambiguity in law is explained below. While some freedom in relation to applying law is always present, the following instance shows how a lack of precision in legal application is inevitable.[22] The internal power conferring rules each legal thinker maintains determines how the law is applied.[23] The following law might be read by formalists in a broad-based way to exacting ends that is not in line with the purpose of the law. Alternatively, a legal realist might read the law for its purpose, but misinterpret the law's purpose in a new instance, creating inconsistency in the precedent. In highlighting these problems, the famous thought experiment provides some contexts as to how legal judgements can be aided by algorithmic tools.

Consider the hypothetical statue stating that "all vehicles are prohibited from Gibson Square in Iowa City."[24] The hard question of law here is: how does this law apply to something like a motorized-scooter? Is a motorized-scooter a vehicle? Or in the spirit of the law, does it really matter if it is a vehicle? Does the statute's purpose merely seek to keep automobiles and larger automated

---

[18] Keenan D. Kmiec, *The Origin and Current Meanings of "Judicial Activism"* CAL. L. REV. 92, no. 5 (2004): 1441, 1442.

[19] In *Second Treatise of Civil Government*, John Locke wrote: "The Legislative cannot transfer the Power of Making Laws to any other hands." Mirroring this, "in *Mistretta v. United States* (1989), the U.S. Supreme Court applied the 'intelligible principle' test. The Court deemed it 'constitutionally sufficient if Congress clearly delineates the general policy, the public agency which is to apply it, and the boundaries of this delegated authority.'"). *See also* IOWA: IOWA LEGISLATIVE SERVICES AGENCY, LEGISLATIVE GUIDE TO SEPARATION OF POWERS (2005) https://www.legis.iowa.gov/DOCS/Central/Guides/lgseppwr.pdf (last visited May 12, 2019).

[20] "Full Faith and Credit shall be given in each State to the public Acts, Records, and judicial Proceedings of every other State." Article IV: STATES, CITIZENSHIP, NEW STATES, CONSTITUTION CENTER https://constitutioncenter.org/interactive-constitution/articles/article-iv (last visited May 12, 2019).

[21] Many of the leaders in choice-of-law theory are academics because judges as theorists only have the ability to access their own single jurisdiction, were professors have the ability to scan the landscape and see it is starving for improvement.

[22] The idea is to use this experiment in the context of technological appropriation of law is not my own. *See* Paul Gowder, *Is Legal Cognition Computational? (When Will DeepVehicle Replace Judge Hercules?)* https://osf.io/preprints/lawarxiv/gk2ms.

[23] "Power-conferring rules differ from mandatory norms with respect to their structure, the way in which they contribute to their addressees' practical reasoning, and their impact on social life." Manero J.R. Atienza M., *Power-Conferring Rules* IN A THEORY OF LEGAL SENTENCES, Vol 34. 44,44 (1998).

[24] Paul Gowder, *Is Legal Cognition Computational? (When Will DeepVehicle Replace Judge Hercules?)* https://osf.io/preprints/lawarxiv/gk2ms, citing Hart (1958).

transportation systems, like golf carts, out of the park? And how would we even find the purpose of the statute, and if we can, how would the judge be able to determine it is the purpose of the law to honor? The judge could decide only two ways in this seemingly simple case—but make the choice from many different reasons.

This is when ambiguity in the application of the law to the unforeseen facts many times leads to imprecise, as what conflict of law scholars deem, "unprincipled" results.[25] One judge might rule that the scooter is a vehicle because it has a motor and is loud and following her interpretation of the purpose of the law, the scooter violates the peaceful park purpose. Another judge might decide that based on precedent, the scooter is not considered a vehicle because a motorcycle was determined not to be a vehicle in another setting. A variety of these concerns could provide a variety of answers.[26] The example shows a need for further "methodological experimentation" for what on its face looks to be a simple, uncomplicated legal issue.[27]

In terms of solutions, theory may now be able to adequately be manifested due to modern programming technology. A theoretical experiment to solve this problem of law has been proposed by jurisprudential scholar Ronald Dworkin where adjudication in hard cases should be interpretive, based on the political mores of the particular jurisdiction. As such, "judges should decide hard cases by interpreting the political structure of their community in the following, perhaps special way: by trying to find the best *justification* they can find," limited by constitutional parameters.[28] A successful interpretation in a difficult case thus is not only the law, but what was meant by the law by that particular society: an "interpretation must *fit* with those practices," aided by "existing legal materials defining the practices."[29] Thus, instead of a judge-preformed research and balancing test on policy, many times which is only directed by the limits of the judge's own mind and experiences, an algorithmic legal approach would better aid in providing the parameters for the judge's decisions.[30] In this way, if the state's legal material such as precedent contained indicators of valued judgements for a strict, formalist, application to the law regardless of reasonableness, this characteristic would be programmed into the algorithm for fit. Likewise, a realist state could embody parameters in the

---

[25] Larry Kramer, *Choice of Law in American Courts in 1990: Trends and Developments*, 39 AM. J. COMP. L 465 (1991) (indicating that the Second Restatement "invites post-hoc rationalizing of intuitions . . .").

[26] James Q. Whitman, *No Right Answer* IN JOHN JACKSON, MAXIMO LANGER AND PETER TILLERS, EDS., CRIME, PROCEDURE AND EVIDENCE IN A COMPARATIVE AND INTERNATIONAL CONTEXT: ESSAYS IN HONOUR OF PROFESSOR MIRJAN DAMASKA (2008) 371, 371 (noting that American law's "reluctance to 'seek' right answers," but instead toil over good arguments).

[27] Paul Gowder, *Is Legal Cognition Computational? (When Will DeepVehicle Replace Judge Hercules?)* 1, 2 (2018) https://osf.io/preprints/lawarxiv/gk2ms.

[28] *Philosophy of Law*, INTERNET ENCYCLOPEDIA OF PHILOSOPHY, https://www.iep.utm.edu/law-phil/ (last visited May 12, 2019). This first idea of societal fit is the most relevant for this paper. Dworkin also proposes a "best morality" prong of judicial interpretation, which if adhering closely to the first prong of fit, is almost nonetheless engulfed by fit. *Id*.

[29] *Id.*

[30] With "hard cases," those where the law does not readily apply to the facts at hand, "judges often invoke moral principles that Dworkin believes do not derive their legal authority from the social criteria of legality contained in a rule of recognition." *Philosophy of Law*, INTERNET ENCYCLOPEDIA OF PHILOSOPHY, https://www.iep.utm.edu/law-phil/ (last visited May 12, 2019).

algorithm that aid in decision making that adheres most closely to legislative intent, based on fit indicators of precedent and also legislative history.[31]

II. Legal Ambiguity in Conflicts

a. Choice-of-Law

Choice-of-law refers to the area within Conflicts of Law where the court determines whether to apply the forum state law or to apply the law from another jurisdiction.[32] Classically, courts with a choice-of-law issue choose between the 1) laws of the state where the lawsuit was brought, and 2) laws of the state where the cause of action arose. The three basic types of approaches to guide these are decisions traditional vested rights doctrine, interests' approach and the most significant relationship theory.[33] This paper will focus on the first two approaches, described more below.[34]

b. Historical Trend Created Ambiguity

In contrast to tradition legal ambiguity, the end of the analysis for choice-of-law is not in sight by determining how to deal with facts that do not precisely line up with the law. There are more complications and legal questions.[35] Some even call the disarray emanating out of this legal area to be "unsophisticated, unthoughtful, and often unreasoned,"[36] where conflicting "theoretical underpinnings of decisions in the same jurisdiction is also common."[37] In sum, the current state of choice-of-law theory has been compared to "revolutionaries" who unite "only to eliminate the existing government."[38]

The sense of ambiguity is compounded by a few factors. First, complexity results from the fact that each of the Restatements are completely different in structure and contents, all of which were driven by legal academia at that time.[39] Additionally, few courts have a multitude of choice-of-law issues, and

---

[31] Technologically program the intent of the lawmakers would be extremely helpful and will be discussed in Part IV.
[32] "Vested Rights Doctrine" US LEGAL https://civilprocedure.uslegal.com/choice-of-law/approaches-to-choice-of-law/vested-rights-doctrine/ (last visited May 13, 2019).
[33] *Id.*
[34] The "most significant relationship" theory is where the judge determines which state has the "most significant relationship" to the case. Aspects such as place of injury, place of the conduct causing injury, residence or place of business of the parties, and the place where any relationship between the parties are weighed. "Approaches to Choice of Law", US LEGAL https://civilprocedure.uslegal.com/choice-of-law/approaches-to-choice-of-law/ (May 13, 2019). The ideal choice-of-law algorithm may successfully encapsulate this doctrine as well, but for demonstration purposes, it is left out of this paper.
[35] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 269 (3rd) (2002) (signaling that "the current choice-of-law theory is marked by eclecticism and even eccentricity").
[36] Larry Kramer, *Choice of Law in American Courts in 1990: Trends and Developments*, 39 AM. J. COMP. L 465 (1991) (indicating that the Second Restatement "invites post-hoc rationalizing of intuitions . . .").
[37] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 270 (3rd) (2002).
[38] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 270 (3rd) (2002).
[39] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 180 & 220 (3rd) (2002) (describing both the first and second Restatements).

therefore never have a chance to develop robust doctrine.[40] Additional complexity is introduced by federal constitutional mandates[41] in relation to the choice-of-law, along with the introduction of alleging multiple types of legal claims in one suit, complicating the characterization of the legal issue. Compared to legal ambiguity in the motor-scooter question, within the framework of choice-of law-problems, ambiguity is instead a question of which law to apply, not just how to apply the law to the facts. In both settings, the evaluation is *ex post*[42] but in a choice-of-law space, federalism forces a judge to carefully examine each potential state law.[43]

i. Vested Rights

Starting from the beginning, the nature of choice-of-law doctrine from its genesis has been reactionary. Since the end of the 16th century, international trade made it "impossible to avoid the problems of conflict of laws forever,"[44] bringing an "influx of conflict cases for which adequate authority did not exist"[45] so thus some solutions were proposed through the First Restatement.[46] As early choice-of-law "developed haphazardly, on a case-by-case basis,"[47] a doctrine of vested rights emerged, perpetuated by Justice Joseph Story and Professor Joseph Beale.[48] Subsequently enforced by Justice Holmes, the vested rights theory was "universally adopted."[49] The traditional vested rights doctrine comes from the idea that the state has the power to prescribe the rules of conduct on its territory.[50] The rights "vest" when the last event of the transaction or occurrence takes place.[51] Therefore, using this approach, the First Restatement consisted of hard and fast rules. To combat any problematic decisions, the vested rights approach is coupled with a wide array of escape devices.[52] Using these options as a means with

---

[40] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 270 (3rd) (2002).
[41] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 1 (3rd) (2002).
[42] Beale, *Summary Conflict of Law* (stating that "no legal right exists by nature. . .the creation of a right is therefore conditioned upon the happening of an event").
[43] "Full Faith and Credit shall be given in each State to the public Acts, Records, and judicial Proceedings of every other State." Article IV: STATES, CITIZENSHIP, NEW STATES, CONSTITUTION CENTER, https://constitutioncenter.org/interactive-constitution/articles/article-iv (last visited May 12, 2019).
[44] *See* Joseph Story, COMMENTARIES ON THE CONFLICT OF LAWS 4 (1834) (noting that "[c]ommerce is so absolutely universal among all countries").
[45] David F. Caveers, *A Critique of Choice of Law Problem*, 47 HARV. L. REV (1933).
[46] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 177 (3rd) (2002). When "American courts first began to be confronted with cases involving the problem, there were so few phenomena in the way of decisions to describe that there could hardly be said to be well recognized principles and rules…courts found themselves on a largely unchartered sea." Walter W. Cook, *The Logical and Legal Bases of the Conflict of Laws*, 33 Yale L.J. 484 – 488 (1924).
[47] *Id.*
[48] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 57 (3rd) (2002). *See also* Joseph H. Beale, *A Treatise on the Conflict of Law* (1935).
[49] *Id* at 6. Herma Hill Kay, et. al., *Conflict of Laws Cases-Comments-Questions*, 5 (2006); *See also* Joseph Story, COMMENTARIES ON THE CONFLICT OF LAWS 4 (1834).
[50] *Vested Rights Doctrine*, US LEGAL https://civilprocedure.uslegal.com/choice-of-law/approaches-to-choice-of-law/vested-rights-doctrine/ (last visited May 13, 2019).
[51] *Vested Rights Doctrine*, US LEGAL https://civilprocedure.uslegal.com/choice-of-law/approaches-to-choice-of-law/vested-rights-doctrine/ (last visited May 13, 2019).
[52] *See* William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 191-202 (3rd) (2002).

which to deny the doctrinally-prescribed law, judges could choose a different law if the original outcome was divergent to the forum state's policy.

ii. Interest Analysis

Interest analysis provides a less rigid approach that adheres to case-specific legal interest. Professor Brainard Currie articulated this "government interest analysis" approach to conflicts.[53] This approach is a "flexible, policy-oriented framework."[54] The "interest" is that of the forum state for the particular objective of the law applied. In taking this interest, this approach weighs the interest against that of other law of states involved.[55] The "comparative impairment" test is used by the court to compare the extent of damage that application of one or the other legal rule to the case would inflict on the competing states interest. Paralleling utilitarian theory, the court would in such cases choose the law that causes the lesser degree of impairment. Currie's ideas stemmed from his conclusion that true conflicts are only those in which interest in the law of the states are at conflict.[56] Where there is no impairment to the other state by the application of the forum state's law, then there is no conflict.[57]

c. Two Seminal Cases

In drawing out a sense of the type of conflicts that occur, two seminal cases have been used as proxies for scholarship in choice-of-law. The first is a tort case,[58] where an injury occurred in one state, but the breach of duty occurred in a different state.[59] In *Alabama Great Southern R.R. Co. v. Carroll*, the conflict was thus regarding the choice-of-law in tort: should the judge apply the law where the breach of duty occurred, or where the injury occurred? Ultimately, the court found that when seeking damages for a breach of duty, the action may be brought only in the state where the *result* occurred. How did the court come to this conclusion? Which normative conclusions created this ruling?

Milliken v. Pratt is another key case conflict scholars use because it was one of the first in which the judge had to decide whether or not to enforce a contract that is valid in the state where it was made, but where it was invalid in the forum state.[60] According to a Maine statute enacted in 1866, a married

---

[53] Brainerd Currie, *Notes on Methods and Objectives in Conflict of Laws*, 1959 DUKE L.J. 171, 176.
[54] *Id*.
[55] "Approaches to Choice of Law", US LEGAL, https://civilprocedure.uslegal.com/choice-of-law/approaches-to-choice-of-law/ (May 13, 2019).
[56] *Id*.
[57] Like vested rights, public policy is used a reason for judges to negate the law of other states.
[58] Carroll lived in Alabama was injured in Mississippi due to a defective railroad link. The court found that the railroad's employees were negligent in their duty to inspect, and the negligence occurred in Alabama. Carroll sued the Railroad in Alabama under a state statute that authorized recovery. As Mississippi would have denied recovery because it had no similar statute providing recovery. *Alabama G. S. R.R. v. Carroll*, 97 Ala. 126, 11.
[59] *Id.*
[60] Pratt was a resident of Massachusetts and signed a guaranty for the benefit of Milliken, who was her husband's creditor. At the time of the signing Massachusetts law stated that she was not able to be a signatory of the contract because of her gender, although no such provision existed in Maine at the time. See generally *Milliken v. Pratt*, 125 Mass. 374 (1878).

woman could bind herself by contract but in Massachusetts, a married woman could not bind herself by contract.[61] Thus, the judge answered the question of a contract's validity within one state against the citizens of another state where such contracts are statutorily invalid.[62] Ultimately, the judge decided that a contract that is valid by the law of the state where it was made is enforceable everywhere, including states where such contracts are invalid by statute.[63]

In overturning the initial decision ultimately for the defendant, the judge found credibility in this decision by distinguishing the suit as a contract case. Acknowledging the initial question of domicile,[64] he stated "the law of the domicile, regulat[es] the capacity of a person, accompanies and governs the person everywhere. This statement, in modern times though, is subject to many qualifications."[65] Most notably is a qualification of character of suit compared to a strictly domicile-based legal analysis. Domicile is the "connecting factor which links a person with a particular legal system, and the law of his domicile is his personal law."[66] At common law, a married woman was presumed to have the same domicile as her husband,[67] so the law that would govern her signing of the contract would have thus been the Massachusetts law. Instead, by characterizing the suit as a contract matter, the judge qualified this choice-of-law dispute as one which contract laws took the lead. The offer of a contract was effectuated when signed, and accepted in Maine by the offeree, and thus it was fully formed in Maine.[68] While this might have been an ingenious solution for 1878, many cases today are presented both with contract and tort claims. The algorithm below nonetheless supersedes the need to deliberate a characterization for legal claim.

d. Constitutional Restrictions

One of the mandatory limitations on choice-of-law is the Constitution.[69] The question here is whether the Constitution permits the state to apply a law. As most states adopt the doctrines of the United

---

[61] *Id.*
[62] See *Id.*
[63] *Milliken v. Pratt*, 125 Mass. 374 (1878).
[64] The determination of a client's domicile is the threshold question in determining many of the rights and obligations of the parties. Domicile is a legal construct that describes the relationship between an individual and a particular locality or country. Robert C. Lawrence III & Elisa Shevlin Rizzo, *Basic Conflict of Laws Principles*, AMERICAN BAR ASSOCIATION 1, 4 (1999) http://apps.americanbar.org/abastore/products/books/abstracts/5430661_chap1_abs.pdf.
[65] *Milliken v. Pratt*, 125 Mass. 376 (1878). "The court specifically rejected, on pragmatic grounds, the suggestion that such a question of capacity to contract should be decided in accordance with the law of the domicile." Brainard Currie, *Married Women's Conflicts: A Study in the Conflict-of-Laws Method*, 25:2 CHICAGO L. REV. 227, 228 (1958) https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=3055&context=uclrev.
[66] J. G. Collier, *Domicile and residence*, UNIVERSITY OF CAMBRIDGE (June 2012) https://www.cambridge.org/core/books/conflict-of-laws/domicile-and-residence/D11CBD36FBB4E5B0EEC617D475D8179F.
[67] Robert C. Lawrence III & Elisa Shevlin Rizzo, *Basic Conflict of Laws Principles*, AMERICAN BAR ASSOCIATION 1, 4 (1999) http://apps.americanbar.org/abastore/products/books/abstracts/5430661_chap1_abs.pdf.
[68] This follows the mailbox rule in contracts, "the default rule under contract law for determining the time at which an offer is accepted," where an offer is considered accepted at the time and place that the acceptance is communicated. *Mailbox Rule*, CORNELL https://www.law.cornell.edu/wex/mailbox_rule (last visited May 19, 2019).
[69] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 296 (3rd) (2002).

States federal constitution, judges in each state are limited by the Due Process Clause, Full Faith and Credit Clause, the Commerce Clause, Equal Protections Clauses, and what is left of the Privilege and Immunities Clause.[70] The impact of full faith and credit and due process for choice-of-law are described below.

i. Federalism

The aim of the Constitution, and of federalism generally, "is to knit the discrete sovereignties of the states into a federal union, and this purpose obviously requires rules governing the treatment of the laws, and the citizens, of sister states."[71] It is tempting to simply negate the power of the states to create differentiating laws, especially when content of the laws have a propensity to involve multiple states. Yet, a "federal common law"[72] can "never correspond to the realities of judicial administration," because judges help enforce the particularities of each state.[73]

The reason federalism is mandatory and should sought to be enforced is inherent in the text of the Constitution.[74] The Constitution is a document outlining the boundaries of the federal government.[75] In it, Article X states that "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."[76] Formally this presumes a difference in the kind of laws, and that there be differences, between the States' laws and the Federal government's laws. These laws formulated by the states are known as "police powers," and each state maintains a culture distinctly different that influences differences in the manifestations of police powers.

As such, Article IV is devoted to the relations between the states and the Federal government.[77] The Full Faith and Credit clause makes it necessary for judges to enforce the law of other states when

---

[70] Robert A. Lefr, *Constitutional Limits of Free Choice of Law*, 706, 707-708 (1959) https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2978&context=lcp. See also *Allstate Ins. Co. v. Hague*, 449 U.S. 302 (1981) (detailing the due process limits on choice-of-law decisions).

[71] Kermit Roosevelt III, *The Myth of Choice of Law: Rethinking Conflicts* (1999) 2448, 2504. http://scholarship.law.upenn.edu/faculty_scholarship/1340.

[72] Courts do not have the judicial power to create general federal common law when hearing state law claims under diversity jurisdiction. *Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938).

[73] Hessel E. Yntema, *The Hornbook Method and the Conflict of Laws*, 37 YALE L.L. 468, 477.

[74] See *Federalism*, PBS, https://www.pbs.org/tpt/constitution-usa-peter-sagal/federalism/#.XNtXpI5KjIU (last visited May 20, 2019). Chief Justice John Marshall noted that the tension between stated and national government "is perpetually arising, and will probably continue to arise, as long as our system shall exist." *Id*.

[75] For example, Article I states that: "All legislative powers herein granted shall be vested in a Congress of the United States."

[76] The Founders granted the national government only limited and enumerated powers and left the regulation of intrastate commerce to the states whereas state legislative powers limited by their own constitutions. Randy E. Barnett & Heather Gerken, *Article I, Section 8: Federalism and the overall scope of federal power,* CONSTITUTION CENTER (July 6, 2016) https://constitutioncenter.org/blog/article-i-section-8-federalism-and-the-overall-scope-of-federal-power/.

[77] Ariela Gross & David R. Upham, *Common Interpretation Article IV, Section 22*. CONSTITUTION CENTER, https://constitutioncenter.org/interactive-constitution/articles/article-iv/article-iv-section-2/clause/37 (last visited May 13, 2019).

appropriate.[78] Full Faith and Credit though does not resolve conflicts by its own force automatically.[79] Thus how to enforce these constitutional provisions is a pertinent question for choice-of-law doctrine: "[h]ow to determine when [federal considerations] require the law of the forum to give way to the law of another state seems to me an unsettled question ... The ultimate answer … [should] be based on considerations of state relations to each other and to the federal system."[80] As it stands, though, the restatements have also not yet resolved the choice-of-law problem.

Both vested rights and interest analysis approaches threaten constitutional protections. Where vested rights appear too rigid to apply amongst an interstate-based modern economy, some claim that "[i]nterest analysis has done a disservice to federalism."[81] Vested rights maintains the ideals of each state where the relevant legal facts were based. By contrast, interest analysis exposes the judge to a case-by-case analysis on what the interest could be of each state. Essentially, this option creates almost a federal doctrine in itself where judges across the board are allowed to identify the motivation of each law, despite collecting little evidence to conclude each interest. Both options have the public policy escape route, which invariably has the potential to deny the full faith and credit of the applicable law. Permitting the escape routes and interests analysis threatens the integrity of each state's law with the implicit federal force in choice-of-law.

ii. Due Process

The Fourteenth Amendment of the Constitution limits judges' flexibility in determining choice-of-law.[82] Most obviously, when a dispute has no connection to a given state, then under the Fourteenth Amendment, it is unconstitutional to apply the law of that state.[83] But when there is ambiguity in the law to apply, the notice requirement of the due process clause mandates that the government be "reasonably certain that the state has some basis for exerting this power," when "a considerable exercise of power is involved in asserting authority to attach one's own normative standard to specific persons or events."[84] The sporadic arbitrary nature of choice-of-law doctrine at times meets the "minimum, threshold justification for asserting normative authority" before invading "another state's interest."[85] Due process in a conflict of laws case is extremely difficult though when legislative and common-law policies underlying specific rules are often unarticulated. Courts simply try their best but

---

[78] FULL FAITH AND CREDIT ACT, 28 U.S.C. § 1738 (1994). *Hughes v. Fetter*, 341 U.S. 609, 611 n.4 (1951).

[79] Kermit Roosevelt III, *The Myth of Choice of Law: Rethinking Conflicts* (1999) 2448, 2453. http://scholarship.law.upenn.edu/faculty_scholarship/1340.

[80] *See* Robert H. Jackson, *Full Faith and Credit: The Lawyer's Clause of the Constitution*, 45 COL. L. REV. 1, 28 (1945).

[81] P. John Kozyris, *Postscript: Interest Analysis Facing Its Critics—And, Incidentally, What Should Be Done About Choice of Law Products Liability*?, 46 Ohio St. LJ. 569-581 (1985).

[82] *Approaches to Choice of Law*, US LEGAL, https://civilprocedure.uslegal.com/choice-of-law/approaches-to-choice-of-law/ (May 13, 2019).

[83] *Id.* (indicating though that "the requirement of connection is minimal").

[84] Frederic L. Kirgis Jr., *Roles of Due Process and Full Faith and Credit in Choice of Law*, 62 CORNELL L. REV. 94, 96 (1976) http://scholarship.law.cornell.edu/clr/vol62/iss1/3.

[85] Frederic L. Kirgis Jr., Roles of Due Process and Full Faith and Credit in Choice of Law, 62 CORNELL L. REV. 94, 96 (1976) http://scholarship.law.cornell.edu/clr/vol62/iss1/3.

often must "speculate and, one sometimes suspects, engage in some creative juggling of policies to reach the desired result."[86] Thus, a system with which to mandate and keep track of such policy rational would be helpful in maintaining due process for conflicts of law cases.

e. Resolving Choice Ambiguity with an Algorithm

Due to this wild west of contradictions and immature doctrine, if choice-of-law has any chance at developing a reliable framework it must be proactively discerned. This framework should honor the differences between states' policy preferences by using some kind of technological solution to harness the confusion. By using a programming tool to limit the scope of a potential decision, the algorithm could help judges by guiding their decisions in choice-of-law by creating a range of options from which to choose while also limiting their decisions to an appropriate range based on precedent, public policy, and other values discussed below. In gleaning the disordered nature of choice-of-law doctrine, compiling all the cases, facts, and other normative measures is reminiscent of what a computer is designed to do: make sense of a wide variety of facts in an accurate and quick manner.[87] In comparing computers to the human mind, it is "essentially impossible to completely process all relevant data or its potentially relevant dimensions. It is just too much.[88] Human reasoners have well-documented cognitive biases, such as the availability heuristic, optimism bias, anchoring, conformation bias, illusion of validity and frequency illusion."[89] An algorithm specific to each state's particular precedent, preferences, and policies could help in this seemingly impossible task.

There is not an impossible situation here though. Because most algorithms do the job that law is designed to do, taking inputs such as facts and normative directions and outputting a result based on those inputs, a mechanical jurisprudence could quite possibly make sense in modern times.[90] An algorithmic tool would help to cease the temptation to produce inconsistent doctrine, based off what many would deem mere conjecture at its worst, and judicial personal preferences, at best. The law maintains no one omniscient entity, not even the Constitution, that provides full guidance on this issue. In turn, legal computer programs would not necessarily function as the all-seeing-eye to determine one legal outcome. The function of the program would simply limit a set of outcomes properly within the

---

[86] *Id*. at 97.

[87] Paul Gowder, *Is Legal Cognition Computational? (When Will DeepVehicle Replace Judge Hercules?)* 1, 3 (2019) https://osf.io/preprints/lawarxiv/gk2ms.

[88] Computers "more cheaply and more comprehensively generalize the prior cases without my biases and idiosyncrasies." *Id.*

[89] Daniel Martin Katz, *Quantitative Legal Prediction—or—How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry*, 929, 26:4 EMORY L. J. (2013) http://law.emory.edu/elj/content/volume-62/issue-4/contents/quantitative-legal-prediction%20.html.

[90] Ultimately choice-of-law is a significant doctrinal area in which to examine the use of algorithms in law because at its core, it is a procedural subject, but variables make the 'algorithm' run to provide a different output. Conflicts is also a good area to examine the use of algorithmic devices in law because the tough cases are. In this way, Conflicts is presumed also to be a procedural topic. Yes, the substance is important. Why else would there be a doctrinal course devoted to the subject? Subject matters, and the contents it guides also matters. Facts and substance may even be dispositive. However, the contents are incidental to the procedure. It, at many times in Conflicts, directs the procedure, but in no way does the substance of the case at hand in a Conflicts guide the entire legal inquiry.

scope of the law and policy.[91] With a set of potential proper outcomes, judges still can use their discretion, it is just limited in scope.

III. Algorithms Applied in Law

a. Computer Science Mechanics, Generally

There is no single consensus for how to describe an algorithm or what makes it a good one. Yet, generally, when computer scientists create programs, the algorithm connects the *abstract how* to the computer code, to perform a desired result. As stated above, this process is strikingly similar to what law does. One of the key differences between law and a program is that computer algorithms can compute much quicker than the human mind.[92] Another key difference is that algorithms always work! When an algorithm provides an answer, it is always correct.[93] These tools are so powerful that computing has transformed nearly every aspect of modern life; one space still to be captured is judicial reasoning.[94]

In developing a lay understanding of how these systems work, computer scientists denote five properties of an algorithm. Each program must be input specified, output specified, definite, effective, and finite. First a computer program is given information that is exterior to the program itself. This is called the input. An algorithm has zero or more inputs, which are essentially the quantities which are given to it initially before the algorithm begins.[95] In the same way, outputs are designed specifically to be limited to the useful information the user of the program will need based on running the program. An algorithm has one or more outputs, which are the quantities with a relation to the inputs.[96] Third, the quality of definiteness describes the level of precision for each part of the algorithm. Each step of an algorithm must be precisely defined; the actions to be carried out must be rigorously and unambiguously specified for each case.[97] Then, an algorithm must accomplish the task at hand. Therefore, effectiveness is a standard expectation in computing. This means that all the operations to be performed in the algorithm must be done exactly and in a finite length of time.[98] Lastly, it is theoretically preferred that the function must end. Thus, finiteness portrays the idea that an algorithm

---

[91] Jason Morris, *How programming can make the law more accessible*, TEDxUAlberta (May 8, 2018) https://youtu.be/d5Mt-Q9K7tU.

[92] Algorithms are also usually used for efficiency. *What is an algorithm and why should you care?* Khan Academy https://www.khanacademy.org/computing/computer-science/algorithms/intro-to-algorithms/v/what-are-algorithms (last visited May 5, 2019).

[93] *Id*.

[94] *Early Computing: Crash Course Computer Science #1*, CrashCourse (Feb. 22, 2017) https://www.youtube.com/watch?v=O5nskjZ_GoI&list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo&index=2.

[95] Nidhi Gupta, *Algorithm and its characteristics*, (Sept. 26, 2016) http://bisma.in/algorithm-and-its-characteristics/.

[96] *Id*.

[97] *Id*.

[98] *Id.*

must terminate after several steps.[99] Sometimes this limiting principle of the output of computations is said also to be a program made in a "deterministic fashion."[100]

The *parts* of an algorithm determine how it works. The programmer fits different pieces, or tools like a puzzle, together in order to achieve the desired result.[101] A first part of the algorithm is the *variables*. Variables can either be primitive, which means that they are those which are already exist as a basic tool within the programming language system, or unique, which means that they are unique to this situation. Variables are used as devices that represent the nouns in the programming syntax. Variables can also be assigned different values and can be limited by parameters. An example of a variable assignment, k = 5 means that whenever the computer sees "k" it understands the value of "k" to be five. Programs need to do something, not just contain a bunch of variables, so *functions* or *methods*, are the tools with which the algorithm accomplishes its task. Examples of such methods include loops, counting, traversing, and many other kinds of functions.[102] An example is while k = 5, +i. This means when k is determined to be 5 in the correct part of the program, i (which is commonly used as a counting placeholder) adds one (which is represented by the +).

b. Programming Process

Developers, professional computer programmers, follow some generally applicable steps for solving computational problems. These are: 1) Problem definition, 2) Development of a model 3) Specification of an Algorithm 4) Designing an Algorithm 5) Checking the correctness of an Algorithm 6) Analysis of an Algorithm 7) Implementation of an Algorithm 6) Program testing 7) Documentation.[103] Programming development problem specification is one of the most difficult tasks because most often the user is not completely clear what the problem is to solve. However, all other work beyond this step will be futile if the developer is not clear about what she wants the algorithm to do.[104] Conversation amongst those involved is a good way to gain clarity around a problem definition.

Then, steps 2 – 6 are typically done through pseudocode. Pseudocode is a way to combine the language we use every day, English, with the functions that the developer knows are available in her

---

[99] *Id.*

[100] Frederick Adams, *algorithm*, CAMBRIDGE DICTIONARY OF PHILOSOPHY (2015) https://search-credoreference-com.proxy.lib.uiowa.edu/content/entry/cupdphil/algorithm/0.

[101] Carrie Anne, *Intro to Algorithms: Crash Course Computer Science #13* CRASHCOURSE (May 24, 2017) https://www.youtube.com/watch?v=rL8X2mlNHPM.

[102] For example, the "search" function is a built in method to search an item in a data structure. The "sort" function is a pre-programmed method to sort items in a certain order. Lastly, the "insert" algorithm puts a variable or group of variables into a data structure. https://www.tutorialspoint.com/data_structures_algorithms/algorithms_basics.htm

[103] *Algorithm Design*, TUTORIALS POINT, https://www.tutorialspoint.com/design_and_analysis_of_algorithms/design_and_analysis_of_algorithms_introduction.htm (last visited May 5, 2019).

[104] From firsthand experience, the part of this paper that outlines the precision of a choice-of-law algorithm was definitely the most challenging part of writing this paper.

toolkit.[105] This step is typically written by hand, is sloppy, and undergoes many iterations and edits. Where an algorithm is a formal definition with some specific characteristics that describes a process, the word "algorithm" can be used to describe any high-level task in computer science.[106] By contrast, pseudocode is an informal and often rudimentary, human readable description of an algorithm. Pseudocode's only objective is to describe the high-level steps of an algorithm for any person to understand.[107] This the below example of pseudocode, the English trained reader can have an idea of what is happening in the program, but the developer who drafted it is provided a roadmap with which to develop a computer-language[108] algorithm to have it do what it says. For example:

Pseudocode for an algorithm for Insertion Sort.

Algorithm: Insertion-Sort

Input: A list L of integers of length n
Output: A sorted list L1 containing those integers present in L

Step 1: Keep a sorted list L1 which starts off empty
Step 2: Perform Step 3 for each element in the original list L
Step 3: Insert it into the correct position in the sorted list L1.
Step 4: Return the sorted list
Step 5: Stop[109]

In describing the algorithm proposed for choice-of-law, I will use pseudocode, so a law-trained reader can understand what is going to happen in the algorithm without understanding programming languages or processes.

c. Qualitative Methods

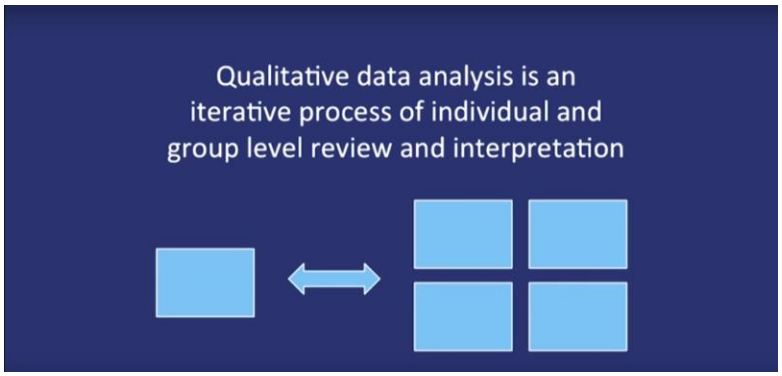
Lastly, it might or might not be obvious that the program above maneuvers through quantitative decisions, but as explained below, legal judgements are not limited by quantitative or Boolean logic.[110]

---

[105] *Algorithm Design*, TUTORIALS POINT, https://www.tutorialspoint.com/design_and_analysis_of_algorithms/design_and_analysis_of_algorithms_introduction.htm (last visited May 5, 2019) (describing pseudocode as "a high-level description of an algorithm without the ambiguity associated with plain text but also without the need to know the syntax of a particular programming language").
[106] *Id.*
[107] *Id*.
[108] Pseudocode is typically not language dependent, though the developer might arrange pieces in specific to the language that will eventually be used, such as C, C++, Java, Python, and other programming languages.
[109] *Linked List*, GEEKS FOR GEEKS https://www.geeksforgeeks.org/data-structure-gq/linked-list-gq/ (last visited May 5, 2019).
[110] Boolean simply means yes/no answer to a question. Marshall Brain, *How Boolean Logic Works*, HOWSTUFFWORKS, https://computer.howstuffworks.com/boolean.htm.

Computers are designed with directions based in 1s and 0s, and numbers are essentially different combinations of these 1s and 0s. Thus, creating a program to evaluate clear cut quantitative issues is cohesive to an algorithm's function. Algorithms then make sense for extremely objective-based decisions, but how do they make sense for one like which law to apply in a choice-of-law matter? And how to apply the choice-of-law? While it is not a clear-cut answer, algorithms are still capable of making these determinations.

An understanding of these issues merits a brief discussion of qualitative research. Despite a less straightforward and single "right answer," in science, there is nonetheless an accurate strategy for "systematic collection, organization, and interpretation of phenomena that are difficult to measure quantitatively."[111] The following image describes a continual process used in qualitative data analysis for the single analyst, or the algorithm, to communicate back and forth with a reviewer and interpreter. For the program proposed in this paper the "other party" is the judge and jury who inserts the initial inputs.



[112]

For example, the law of tort cannot be explained strictly by quantitative measures regarding each of the basic elements: 1) duty 2) breach of duty 3) causation 4) harm. As explained above with the park example, since words are used to define the scope of the law, ambiguity persists. Just as there is a question of what qualifies as a vehicle, there is a complicated qualitatively-based question for determining which elements are satisfied. Likewise, what counts as a duty has many grey-areas. For example, with the duty of care regarding the doctor-patient relationship. Was a duty breached if the nurse was negligent, not the doctor? How negligent does the breaching party have to be? What if the patient dies as a result of a miscommunication by the ambulance driver to the surgery team? Each question or issue based off the simple element that requires a Boolean response (was there a duty? breach, causation, harm Y/N) is based off a finding of fact. This analysis appears to be a process that is

[111] Leslie Curry, *Fundamentals of Qualitative Research Methods: Data Analysis*, YALE UNIVERSITY (June 23, 2015) https://www.youtube.com/watch?v=opp5tH4uD-w.

[112] Leslie Curry, *Fundamentals of Qualitative Research Methods: Data Analysis*, YALE UNIVERSITY (June 23, 2015) https://www.youtube.com/watch?v=opp5tH4uD-w.

simply too complicated to be represented by computer code. However, algorithms do much more complicated levels of analysis than this legal question, so can work with the law.[113] The key to putting law into code is breaking these larger elements of a tort into mini Y/N questions.

As long as the programmer is able to accurately design the potential inputs to mirror the law, the eventual output (an existence or nonexistence of a duty) can be determined. For example, admitted facts may be represented with a Boolean answer, the form of communication used by computers. Was the patient at the hospital 2 hours before the time of death? Was the patient escorted through the ER? All of these answers are Y/N answers. In the most simple form, the total of the these yes's or no's would aid in the algorithm's eventual answer if there is a duty. Thus, if the desired result is well defined and the input is well defined, what appears to be an ambiguous non-deterministic issue can actually be evaluated through tiny methods. The key is the algorithm's focus on the procedure, using logic for "the purpose of achieving a well-defined result from well-defined input."[114] Each step of the algorithm must be connected so what appears to be uncalculatable is broken down into very small pieces in order to make it meaningful to the computer.[115] In this way, each small "step refines the processing towards the desired result."[116]

Although the amorphous nature of subjective legal issues poses a legitimate problem I hoped to cure above, for choice-of-law, the need to start with a qualitative evaluation is even less necessary. Choice-of-law is a procedural matter in its most basic function, where the question is quite literally, "what law do I apply," and "how do I know which law to apply"? Where the substance of the case will determine these answers, the substance of the case is not the focal point of the analysis. Although argued differently elsewhere, the method, or rather the procedure, is the answer here. The question regarding if the state has used vested rights or interest analysis in the past can be read as a Boolean answer. This ultimate answer would come from mini questions regarding how much precedent backs up the particular strategy in for the particular kind of claim.[117] Thus, what appears to be the qualitative parts of the choice-of-law process is thus adaptable to algorithmic code.

d. Applied to the Motor-Scooter

The algorithmic analysis of the Gibson Square problem using computer-friendly notation shows that computers "are just simple machines that preform complex action through many layers of

---

[113] *See* Kevin Slaven, *How Algorithms Shape Our World* TEDTALKS (2011) https://www.ted.com/talks/kevin_slavin_how_algorithms_shape_our_world?language=en.

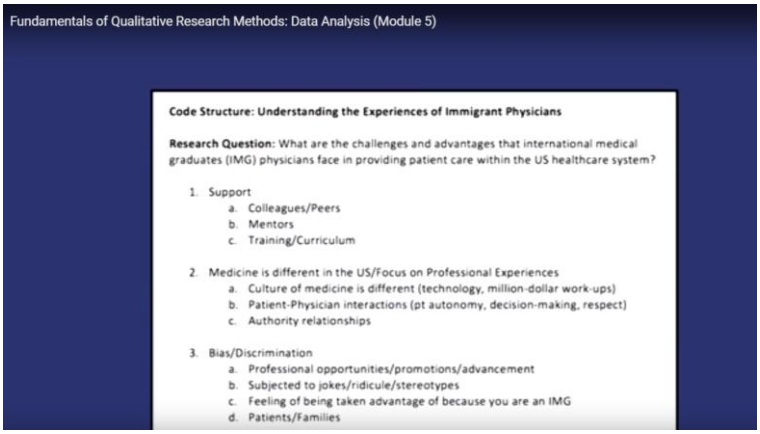
[114] Email conversation, Yvonne Galusha University of Iowa, Tippie College of Business - Management Sciences Dept. (April 11, 2019).

[115] *Id*.

[116] Email conversation, Yvonne Galusha University of Iowa, Tippie College of Business - Management Sciences Dept. (April 11, 2019).

[117] See *Infra* Section III.a for discussion about use of Westlaw Keys to transform legal rulings to numerical computer-readable metrics.

abstraction."[118] In law, by comparison, reaching these layers of abstraction is typically preformed by law clerks and checked by judges. The source of these abstraction-producing parameters are databases such as LexisNexis or Westlaw, each rich with data from key numbers.[119] Therefore, in determining where to start the legal question needs to be presented. ***Is riding a motor-scooter in the park a violation of the law***? In facing this question in the physical context of using the algorithm, law clerks see the question directly imbedded into the graphical user interface. Below is an example of how the algorithm is presented to the user:



120

The questions instead for this legal issue would be the one bolded above. The questions in the system would be included as follows: Was a person in Gibson Park and was the person riding a vehicle? (N/Y/M). If not, the screen would go to a statement on what to do in this matter if a negative result is found. If Yes or Maybe, more questions would be asked regarding the details of the factual situation. In this initial process, the inputs are being carefully delineated.

Once the initial facts are inputted by the clerks, the algorithm applies its internal functions based on the hard-coded inputs which are precedentially-based. The jurisdiction's precedent delineates a realist pragmatic approach, for example. This approach applies in all cases except rulings and statutes regarding cars and boats, where a stricter formalistic approach is used. This initial determination would be based on data collected from sources like Westlaw to indicate a leaning of a pragmatic legal analysis.

---

[118] Jason Morris, *How programming can make the law more accessible*, TEDxUAlberta (May 8, 2018) https://youtu.be/d5Mt-Q9K7tU.

[119] It has been noted that machine learning would require "lots of training data," the inputs for the computer to know where to move next, which "does not exist in any useful form for most areas of law." Although the public domain does not have training data, these companies do have forms of data regarding decisions and legislative history available for both federal and state decisions. *See* Paul Gowder, *Is Legal Cognition Computational? (When Will DeepVehicle Replace Judge Hercules?)* 1, 2 (2019).

[120] Leslie Curry, *Fundamentals of Qualitative Research Methods: Data Analysis*, Yale University (June 23, 2015) https://www.youtube.com/watch?v=opp5tH4uD-w.

The computer would know to apply this type of analysis with the data inside of the algorithm (hard-coded inputs from Westlaw and legislative history) and with the data the user provided (facts of the case, the use of a motorcycle, specifically). Then, with the pre-programmed functions regarding how to deal with such kind of facts applied to the law, the computer would generate an outcome resulting in a pragmatic application of this law. In this way, the scooter-cyclist might be reprimanded to avoid the park during busy times and not to use a scooter that makes a loud noise. Yet because the pragmatist notion of the law applies where safety is the main concern for the law prohibiting vehicles (as determined by legislative history), the algorithm deems the law not to have been violated.

e. Legal Algorithms Provide a Middle-Ground Tool to Transcend the Formalism-Realism Debate

There is a valid concern left with this suggestion of a real-life *Mechanical Jurisprudence*, where a computer program should not allow the practice for judges to clumsily "appl[y] previous precedents to the facts of cases without regard to the consequences."[121] Although the Second Restatement comments mention that "certainty, predictability and uniformity of the result," are "important values in all areas of the law," the drafters admit in line with Pound's cautions that these values can at times be purchased "at too great a price."[122] Therefore, the formalists values should be mediated only to the degree possible, while also adhering to new rules.[123] Where judges have a duty to consider the practical effects of their decisions, a legal algorithmic model would consider not only the formal structure of the law, but the attitudes of society (through the proxy of legislative history) towards a particular legal question. Pound notes the value in formal structure, identifying law as "scientific in order to eliminate so far as may be the personal equation in judicial administration, to preclude corruption and to limit the dangerous possibilities of magisterial ignorance."[124] Yet, law is not scientific for the sake of science, or rather for the sake of the rules themselves.[125]

The formalism-realism debate has been important as a means to dissect the goals in law. And it was an evitable debate: the nature of law written in words creates a broader scope of ends, compared to the ends in science. Professor Sarah Lawsky exhibits the logical discrepancy between the need for an answer in a real situation and gaps or conflicts in statutes, those of which need to be applied.[126] She notes that rules cannot be comprehensively "understood as merely deductive," and that some legal reasoning could be better formalized using default logic.[127] Her point is thus that, for example in statutes, the internal logic is not precise enough to rely on the words and definitions without internal

---

[121] *Mechanical Jurisprudence*, https://www.encyclopedia.com/law/encyclopedias-almanacs-transcripts-and-maps/mechanical-jurisprudence (last visited May 6, 2019).
[122] *Id*.
[123] William M. Richman & William L. Reynolds, *Understanding Conflict of Laws*, 208-209 (3rd) (2002).
[124] *Mechanical Jurisprudence*, ENCYCLOPEDIA.COM, https://www.encyclopedia.com/law/encyclopedias-almanacs-transcripts-and-maps/mechanical-jurisprudence (last visited May 6, 2019).
[125] *Id*.
[126] Sarah B. Lawsky, *A Logic for Statutes*, 21 FLA. TAX REV. 60, 62 (2017).
[127] *Id*. (noting that default logic is "unlike standard logic," more like "defeasible reasoning: default logic permits formal reasoning that results in conclusions that may later be defeated").

rules[128] delineating priority in the chance of ambiguity. Her solution is applying this default logic to statutory interpretation. In the setting of conflict-of-laws, such normative suggestions towards a logical roadmap has already been tried and proposed in each restatement. Instead, a tool, such as the algorithm suggested above, provides a mechanical system to apply the logic of the restatements, but to also keep the decisions in line with the mores of the jurisdiction. Thus, the algorithm simply bolsters the legal decision-making process, eliminating unfairness in some instances by mechanically defining the scope of potential decisions.

Such a mechanical fault-free process takes some human error out of determining the bounds of legal outcomes. Theoretically, an algorithmic approach to law is the best of both worlds. Here adherence to predictable outcomes is obviated, but an adherence to the purpose of the law is also maintained, as the jurisdiction so desires. Where judges are "institutionally constrained from throwing up their hands and saying 'I don't know'"[129] the algorithm provides an opportunity for judges to derive a set of solutions based on a scan of cases from the jurisdiction, while also being sure to "respond to the vital needs of present-day life."[130] This program works as a guide for judges to produce a set of legal possibilities from which the judge may ultimately decide. The outcome provides an output of refined options or even a set of natural language instructions for the judge or jury. The human element is still present in the ultimate legal decision.

V. Choice-of-Law Algorithm

a. Algorithm Proposed

As noted above, algorithms are tools with steps that solve problems. The problem we have here is a doctrinal ambiguity with how to apply a choice-of-law problem once it enters a judge's chambers. The steps below will outline a hypothetical case and describe the work that the algorithm would do in the choice-of-law setting. The prose and graphics will provide a sample overview of how an algorithm for choice-of-law might work. Therefore, the legal evaluation here is not meant to be written in stone, but rather the example here is a framework that enables a full discussion of my proposal for an algorithmic solution to the choice-of-law.

First analyzed is *Milliken v. Pratt*,[131] the seminal contract case.[132] Recall that in this case Pratt (Defendant) was a resident of Massachusetts. He had signed a guaranty for the benefit of Milliken (Plaintiff). Milliken was her husband's creditor in Maine.[133] At the time of the signing, because of her status as a woman and the law forbidding women to enter into contract, she could be technically

[128] Such as rules of recognition.
[129] Gowder at 3.
[130] Pound at 614.
[131] *Infra* Section *III.b*.
[132] See *Id*.
[133] *Milliken v. Pratt*, 125 Mass. 374 (1878).

incapable of entering into such a contract. Yet, this was the law in Massachusetts where she lived. No such disability existed in Maine, where the force of the contract was relevant per the creditor's business. The contract was accepted in Maine. Therefore, when the contract was legally binding, it was physically in the state where the status as a woman would not invalidate the contract. As it was readily accepted, the court found that a contract that is valid by the law of the state where it was made. It held that a contract, including this one, is enforceable everywhere including states where such contracts are invalid by statute.

How did the case come to this conclusion?[134] Essentially, the opinion creates a theoretical hoop to jump through, characterization. Instead of providing judges an open-ended environment ripe with temptation to consider creative legal theories as existential mechanisms to produce their desired result, an algorithm would help judges maintain doctrinal integrity while also considering constitutional choice-of-law issues like full faith and credit. In providing a set of potential outcomes based on a systematic computer-generated analysis of precedent and legislative history, this case might or might not have been decided differently. However, the *reasons*, as lawyers know, for a decision are essential. An algorithm would instead also maintain a state's doctrinal integrity.

This case exhibits, "judicial caprice" which occurs when judges decide to use the escape device of public policy. Public policy provides the judge an opportunity to negate the legal application that could be construed as repugnant to the policy of the state.[135] However, just as arguably excessive judicial discretion is seen in *Milliken*, what is the source of authority for this public policy determination, and what is the limiting principle? Where a lack of answers is provided doctrinally, this algorithm seeks to limit the bounds with which the judge is able to divert from doctrine or choice-of-law, based on a calculus of law and policy (fact) pre-programmed determinations within the algorithm. In this way, the judge cannot be tempted to divert to a ruling that does not make sense for fit.[136]

Rather, the goal of a choice-of-law algorithm would be a mandated process that limits the scope of judges' decisions with an objective to reduce the tendency of judicial opportunism. The secondary goal is to help maintain the differences among states, and our federalist system. This does not mean that there will be no human discretion in legal decision-making if the algorithmic approach is applied, it simply means that the human error and bias is minimized. Where, "[l]aw is not logic, however usefully logic may be made to serve the ends of law [and a system] without careful analysis of the practical purposed of legal traditions and institutions considered with reference to the concrete case is not merely obscurant but socially dangerous,"[137] the algorithm systematically prevents judges' temptation

---

[134] *Infra* Section III.b.

[135] There is a public policy escape device for both vested rights doctrine as well as more modern doctrine as seen in the second restatement. These escape devices that allowed judges to "mitigate the rigidity" of conflicts mechanisms. Kermit Roosevelt III, *The Myth of Choice of Law: Rethinking Conflicts* (1999) 2448, 2497 http://scholarship.law.upenn.edu/faculty_scholarship/1340.

[136] *Infra* Section II.

[137] Hessel E. Yntema, *The Hornbook Method and the Conflict of Laws*, 37 YALE L.L. 468, 477.

to avoid a careful analysis. Legal theorists' critical tone on the choice-of-law doctrine parallel such fear of social danger.

For example, the program could be structured with the following steps. Another part (*b*) will provide precision to the steps in pseudocode. This part is an introduction to the algorithm in abstract form:

Problem Statement

Which law should apply where a choice-of-law argument is possible or proposed?

PART A

USE PROGRAM ONLY if answer YES to this question for the case:

Is there a possibility of a choice-of-law issue, or is such argument made by a litigant?

Below is the ontology[138] that is programmer-generated, but the legal clerks also provide case-specific data.

1) **GIVEN Parameters to Insert by Judicial Clerks:**[139]

Forum State

Other states law in consideration

Parties

Claims (tort, contract, property, etc.)

Legally Relevant Facts

Those agreed upon – Admitted by all parties

Those disputed

Time and place of first occurrence of these facts

[138] *See* Gowder at 4 (discussing the need to determine the initial feature inputs where "we cannot include every piece of knowledge that we have about the whole universe").

[139] This example algorithm and components of the algorithm is not written perfectly, so parameters and details mentioned with this example here are not exhaustive to a choice-of-law algorithm.

2) GIVEN Parameters to Insert by Computer Programmer or Legal Engineer:

Each state's precedent

Each state's legislative history

Each state's policies

These attributes would be pre-programmed so that the relevant procedural questions for choice-of-law are actually implemented and applied directly into the choice-of-law decision-making-process. Additionally, should a public policy question arise, the statutory history needs to be hard-coded.[140]

3) Constitutional Parameters Initially Implemented

The relevant constitutional protections that are automatically provided to citizens, based alone on the facts and law above, should be applied at this stage.

Part B

Decision 1: Any Conflict? → Y/N/M

If there is no disparity in outcomes, then it is the end of the program. For both a vested-rights[141] state law, as articulated in interest-analysis theory, the outcome could be the same despite which state's law is applied. This is a false conflict. Choice-of-law analysis becomes necessary "only when there is a true conflict between the laws of two or more states, each having an interest in the litigation."[142] If there is no conflict, no further analysis is necessary, and the "court will simply apply law of forum state[] when there is no conflict between laws of relevant states on the issues raised."[143] The easy result appears as the ruling if there is no conflict.

Here, the computer internally determines the outcome of each claim based on both vested rights and interest analysis. Then the program compares the outcomes. If there is some disparity between VR outcomes or between IA outcomes, then there is a conflict. This initial analysis uses Currie's true conflict idea as a way to negate a choice-of-law analysis if each track would yield the same result. Proceed to **Decision 2**.

---

[140] These two endeavors are bound to take lots of time and be met with resistance from the Bar and other legal settings. However, such technical application of law to code is presumed to be inevitable, if not in 10 years, at least in 100 years.

[141] This proposal assumes that the vested rights theory is managed by courts in different ways and the discernment in application is bias toward the citizens of the forum. Therefore, for example, in Millikin the vested right could be interpreted as procured in Maine, as was decided in the case. Alternatively, there are a variety of rationale including the cite of last point of control, and others, for the vested right to be reasonably interpreted to had occurred in Massachusetts. Thus, the False Conflict evaluation is used for both methods here.

[142] *Dale v. Ala Acquisitions I, Inc. Eyeglasses*, F. Supp. 2d 423, 428 (May 26, 2006).

[143] *Mumblow v. Monroe Broadcasting, Inc*. 401 F.3d 616, 620 (February 28, 2005).

While the holding could ultimately be the same, the subjective parameters such as damages, could be understood and evaluated by the judge by these descriptions of the law. Yet, the final decision, or set of potential optional decisions, are the output for the algorithm in this case.

Decision 2: **Vested Rights State or Interest Analysis?**

For this decision, choice-of-law precedent would dictate that the forum state would either fall into the vested rights or interest analysis category. This is a determination that would be pre-set by the algorithm based on the prior precedent of the forum state.[144] This is pre-set as to honor the legal decisions for each jurisdiction, determined by the ontology given, prior to the new case's particular use. Some states might depart from one of these approaches for certain kinds of cases, and by using precedent, that will also be honored with this decision. The reason the forum state was chosen here is that judges in that state should be applying the choice-of-law procedural doctrine of their own jurisdiction.[145]As such, each forum jurisdiction would already be set as either a vested rights state or interest analysis.

1) IF VR in forum RESULT → *program uses vested rights algorithm*.

Here the legal algorithm would be programmed to honor vested rights doctrine. Vested rights means that the law to apply is the legal rights "vested" with regard to those at the time that those facts occurred. The court's task is to determine and enforce the law that applied to a set of facts and the rights created under that law according to the time of the occurrence of those facts.[146] Then based on this standard, the program proposes a set of holdings, or one option.

2) IF INTEREST ANALYSIS in forum RESULT → *program goes to interest analysis option.*

The algorithmic mechanisms of interest analysis work similarly as that above steps of vested rights analysis but with some more steps. For government interest doctrine "courts [] use the norms of the state with the greatest governmental interest in the outcome of the particular issue as it guides to decision."[147] Here, the pre-programmed information provided by the algorithm's ontology in Part 1 enables a comprehensive articulation of particular state interests, particularly through the window of legislative history and precedent. Once the program decides the interests, it weighs the interests between each state to determine which law would be most pertinent to apply. The options are

[144] An alternative to this route is creating different categorical options for each particular legal claim as a first step, then determining if there is a vested-rights of 2nd Restatement doctrine in the jurisdiction for that particular category of law.
[145] "Usually a law of state where the lawsuit was brought is chosen for procedural matters." *Approaches to Choice of Law*. US Legal. https://civilprocedure.uslegal.com/choice-of-law/approaches-to-choice-of-law/ (May 13, 2019).
[146] Perry Dane, *Vested Rights, "Vestedness," and Choice of Law*, 1191, 1194 (1987) https://digitalcommons.law.yale.edu/fss_papers/3993.
[147] Harold G. Maier, *Finding the Trees in Spite of the Metaphorist: The Problem of state Interests in Choice` of Law*, 56 ALBANY L. REV. 753, 754 (1993). This is much like Dworkin's suggestion to use the social mores of the jurisdiction for tough decisions.

provided, and options of law that are in a deficient interest due to the applied law are eliminated. The best options with the highest interest level manifested are proposed.

Decision 3: Decision Scope Narrowing

1) Constitutional Limits

The scope of possible decisions is first potentially narrowed with a Constitutional law check. The documents of relevance for this task include both the federal Constitution of the United States as well as state constitutions.[148]

2) Escape Routes

Finally, escape routes cover the instances when a "conflict of laws rule may be disregarded when the foreign law it selects dictates a result repugnant to the public policy of the forum."[149] This approach has been deemed be a "somewhat cavalier dismissal of a foreign law" because "it dispenses with the necessity for close analysis[and] for affirmative appraisal." Instead here, the computer program systematically brings in public policy considerations based on the combination of the potential rulings from the conflicted outcomes per **Decision 2** with the public policy of the forum state. Each public policy consideration from the ruling would interact with the algorithm's findings from legislative history.[150]

As legislative history was already a consideration for vested rights analysis, the distilling function here will be more abundant for vested rights decisions. The legislative history is hard-coded and determines public policy. The algorithm then, if the holding is repugnant to public policy of the forum state, outputs the reason for the conflict and suggests a smaller scope of appropriate options.[151] If possibilities arise, this decision ultimately requires deference from the court.[152] Escape routes via policy is applied for both VR and IA, but public policy is the only escape device that retains a prominent role in the 1971 Restatement.

Part C

Ultimate ruling options are provided here.

---

[148] *See* Gowder at 6 (discussing the need for an internal authority-determining hierarchy).
[149] RR 207.
[150] Precedent is of value here as well to determine public policy of a state, but precedent for the fact pattern has already been apply systematically in the algorithm via Decision 2.
[151] For demonstration purposes, this paper treats the public policy escape device as one of many escape devices. Other 1st Restatement escape devices are characterization, renvoi, penal laws and tax claims. *See* Herma Hill Kay et. al. *Conflict of Laws Cases-Comments-Questions*, Table of Contents xv (2006).
[152] (RR-213).

As the algorithm is always right, this also means that there might not just be one right outcome. Legal text is not as precise as numbers where it is undisputable of one right outcome 3 + 3 = 6. Instead the program works like ~3 + ~3 = ~ {4 – 7}. The program would not create 100 as the answer to the second math problem, but quite possibly, where a judge who had read only a handful of particular cases and comes with particular predispositions, might select 100 and nonetheless earnestly believe that she is within the scope of correct options. Therefore, there could be a number of outcomes, just as Jason Morris found with his legal experiment. In his TedTalk, ABA Innovation Fellow, computer scientist who has become an attorney, described an experience regarding computer code and law. Morris set code to an intellectual property case. The outcome, he expected, would be the decision in the case. Yet, the program's output was three different options. Because algorithms are always right, and Morris' code did not take into account the human element of the judge or jury, these potential legal rulings described the logical bounds of potential right answers.

b. Algorithm Explained

These steps are really just parts of a complicated flow chart. The choices become less workable with computer code when there are qualitive determinations to make. The choice-of-law algorithmic answer is nonetheless a set of options from which to pick. In this way, discretion is available but in a principled way, maintaining the integrity of the law.

As shown above, the algorithm suggests no need for a "most significant relationship" analysis from the 2nd Restatement because the suggested algorithm nonetheless provides the outcome this contacts concept seeks to fulfill. Additionally, that since jurisdiction analysis provides a contacts-based inquiry, this theory is not warranted as an additional-basis for choice-of-law. Further, if a significant relationship ruling results in an outcome conflicting the purpose of other states, then the laws risk due process and full faith and credit. The legal decision must be tied to actual states preferences otherwise conflict of laws game is futile. Policies and interest have always been preeminent in choice-of-law analysis, and for constitutional reasons. By comparison, "whether a particular 'contact' is significant is meaningless unless significance is judged in terms of policies and interest of states involved … we are left [again only] with the tools of construction and interpretation."[153]

With the application of the algorithm, would a judge still have autonomy to use an escape device? No, she would not. The judge would only be able to negate the rulings with some other kind of mechanism, much like an egregious verdict and judgement notwithstanding the verdict.[154] This is the practice in American courts whereby the presiding judge a civil jury trial may overrule the decision of a jury and reverse or amend their verdict. It is rarely granted by judges but permits the judge to avoid extreme and unreasonable jury decisions.

[153] Symposium, Comments on *Babcock v. Jackson*, A RECENT DEVELOPMENT IN CONFLICT OF LAWS, 63 COL. L REV. (1963).
[154] RULE 50(B). FEDERAL RULES OF CIVIL PROCEDURE.

Many are uncomfortable with this approach which "anthropomorphizes the state, inferentially characterizing it as a sentient entity with self-generated feelings, thought, and concerns," creating an unprincipled approach.[155] Yet, with a systematic decision-making process used with this algorithm, the sentient entity need not exist. Data from legislative history, precedent, and possibly society, enables the judges to quickly limit the scope of their rulings. The algorithm then works as an accountability system, providing a result of systematized evaluation of information. Where "no evidence exists that the state governmental authorities monitor the manner in which sister state courts decide choice-of-law cases or that any political responses is engendered if a foreign forum incorrectly borrows or fails to borrow a state's local law," the algorithm is a measure to produce data-driven rulings in the absence of "sovereigns whose laws may be applicable and, therefore, whose interests may be at state are not usually represented before the court."[156]

c. Algorithm Applied

Below is an example how the algorithmic approach works on a choice-of-law fact pattern. Using Millikin, the problem here is that the choice-of-law for the forum state would invalidate the contract. Per **Part A**, in this fact pattern it is proper to use the algorithm because there is an answer **YES** for this question: *Is there a possibility of a choice-of-law issue, or is such argument made by a litigant?* The judge needs to decide if the forum state's law is the appropriate law to apply or if the state where the contract was created is the proper law.

Next, the judicial clerks are to provide answers to questions. Each question has options, the selection of which prompts the computer with logical meaning. With the exception of a **Forum State**, which would already be loaded as given Massachusetts, there are a large number of options for these questions. Data to be entered include: **other states law in consideration, demographics of parties, types of claims** (tort, contract, property, etc.), **legally relevant facts and for each fact; *Those agreed upon – Admitted by all parties, Those disputed***. Here the other law in consideration was a Maine, contract law. Demographics of the party are relevant for both application of law, in this case because there was a disparity in one of the laws due to gender, and for constitutional measures such as equal protection. Here, the offeror resided in Massachusetts and was a female. The creditor was a male who lived in Maine, who also was the offeree. The type of claim that the offeree made was a breach of contract claim.

Legally relevant facts would automatically come up on the next page that was pre-programmed with options for both Maine and Massachusetts legally relevant facts. Here for example it is admitted that the contract was signed, and the signatory is a female. Both of these facts are legally relevant and potentially dispositive, but they are undisputed facts. So the clerks should use them as inputs.

---

[155] *Id.*
[156] See *Id*.

Now, instead of the court determining that domicile was an antiquated doctrine and arbitrarily creating a ruling based on institutions of what is best in this instance, in using an algorithm for choice-of-law, the court could have made a principled, and relevant, decision. This would have occurred because the pre-programmed laws and policies from each state. The **GIVEN Parameters to Insert by Computer Programmer or Legal Engineer** could include: Each state's precedent, Each state's legislative history and policy reasoning, Each state's alternative policies. By using these to guide what we know to what we need, the algorithm does not miss any information.

If it was a government-interest state for *Milliken*, it was clear there is a conflict, so then per **Decision 2**, when the Computer Applies the **Fact to Law** to see if there is any conflict it would answer **Y**. Potentially, vested rights state select the creditor and interest analysis would select Mrs. Pratt. With this legal disparity the computer would print out on the screen the logical reason why the conflict exists. Here the judicial clerks would see something like: "For Massachusetts and woman offeror → no contract. Maine → valid contract." The algorithm would calculate the parameters already included by the programmer and determine an answer based on these extra-legal considerations. Here, if the legal precedent and legislative history weighted strongly in favor of forbidding women to have contract rights in Maine and those sources of law also had a weak force for reliance on contracts, then the decision would be suggested to be decided the other way. Here, interest analysis is preformed by the computer instead of the humans who have limited time and resources to precisely calculate the interests.

Finally, the relevant escape doctrines that apply to the law and fact would be exposed by the computer per **Decision 3**. The computer creates a scale to determines the weight of the public policy and other escape routes, indicating if a different law applied would be more salient. If the escape route meets the threshold, the judge has the additional option to apply another law.

d. Algorithm Broadly on the Ground

This system's induction into the American legal system would be a monumental effort, though the effort should be seen as not as a way to "replace judicial reasoning and legal argument," but to augment it.[157] The first question is which parties determine the initial inputs. Professor Susan Morse predicts that disputes will be preeminently among between the makers of automated systems and regulators.[158] Therefore, it would be best if the algorithmic approach in the judicial sphere is not solely a privately-run operation.[159] Conflicts of interests are bound to occur abundantly with legal-

[157] Paul Gowder, *Is Legal Cogitation Computational? (When Will DeepVehicle Replace Judge Hercules?)* (2019).

[158] Susan C. Morse, *Government-to-Robot Enforcement,* ILLINOIS L. REV. 1, 2 (March 19, 2018) https://ssrn.com/abstract=3143716 (noting that "no matter how well-designed an automated law system is, errors are inevitable.").

[159] Where turbo-tax has a special relationship with the government an outside company involved in state's litigation decisions is quite sensitive and privileged. Turbo-tax receives the government's advice if and when errors occur, and if errors occur due to the TurboTax software, the Internal Revenue Service reimburses the applicant. *Id*. at 3.

augmenting software given the opaque nature of programming languages to the lay person. Maybe the American Bar Association or Judicial Conference of the United States should start thinking about creating job pathways and outlets to pave the way for algorithmic legal solutions. Legal engineering is a new line of work, which requires a legal background to understand the law, and computer science skills, to effectuate legal software programs. Where "system designers [] have incentive to favor regulated parties to purchase and use their system," to avoid some aspects of law with loopholes for example, the government should take the reins in developing such projects.[160] In providing a transparent process, the government may also decide to provide citizens or lawyers with the ability to access the algorithm.[161]

VI. Limiting the Limitations

As with every solution, the technologies support law are nonetheless fallible.[162] Bugs, education for lawyers, and increasing the power disparity among citizens, are some issues of concern that might manifest after an algorithmic solution is enacted. Additionally, input and interpretation bias are always subject to occur both with the programmers and judicial chambers. Updating law and overturning law also creates more complications to this idea. And where exactly are the Dworkinian social mores supposed to come from? Where is the line drawn between informative information and legal irrelevance?

Ultimately, an algorithmic way nonetheless provides a middle-ground to transcend the formalist-realist debate. This approach has the capacity to adhere to all the rules that formalists desire the law to follow, but also enables realists' goals in adhering to the actual issue at hand by providing the judge options and discretion within each option. Further, an algorithmic approach to law is appropriately expressed through choice-of-law because this area is procedural in nature. It is also vastly disorganized, so structure would do it some good.

Though, conversely, the who, where, when, and what are still to be determined. The goal of this paper is not to ultimately determine the ultimate solution for conflict of laws, but to note that the tools available to lawmakers are good ones, tools that have enabled precision in other subject areas. These tools have capacity to automatically protect constitutional mandates such as federalism, due process, and full faith and credit.

---

[160] *Id*. at 17.

[161] Paul Gowder, *Is Legal Cogitation Computational? (When Will DeepVehicle Replace Judge Hercules?)* 1, 10 (2019).

[162] Susan C. Morse, *Government-to-Robot Enforcement,* Illinois L. Rev. 1, 16 (March 19, 2018) https://ssrn.com/abstract=3143716 (noting that "no matter how well-designed an automated law system is, errors are inevitable.").

Conclusion

Conflicts is an ideal setting to examine the use of algorithmic analysis of law because it is a process-oriented area and one in which the doctrine requires cleaning. As an anecdote to this problem, algorithms are well-ordered with unambiguous operations.[163] In developing clarity around the limits and bounds of a choice-of-law doctrine, algorithms should have explicitly defined set of inputs and outputs. This essay assumes that the functions underlying the programming code of an algorithmic approach to Conflicts need not be meticulously understood by citizens or lawyers, but what does need to be understood is a precise manner and application of the theoretical inputs and outputs. In this way, choice-of-law questions are accessible to litigants, predictable, and also not influence by extravagant judicial discretion. Where much technological legal theory relies first on technological ideas generated by legal scholars, this paper seeks to demonstrate how automated systems can solve existing legal problems within the law itself with extant tools.[164]

These tools have been around for almost a century[165] but only in the past few years have legal scholars started contemplating the applicability of technology directly to law.[166] Where scientific and even our cousin profession, medicine, has been dedicated to such precision in results, law maintains a mediocre and outdated way to determine legal truth. Computer science, if at all used in aiding legal decision making, has been performed or proposed as a method to help predict judges' decision, interpret natural language, or convince a jury. Yet the way society has documented, referenced, and utilized law, has changed with the times. Appropriate technology to aid in such tasks started with clay tablets, and includes typewritten paper versions of law, along with electronic databases of law. The next step is an algorithmic expression of legal logic and precedent.

While technology has the capacity to replicate or aid in the process of legal application, scholarship examining the feasibility of algorithmic legal analysis in choice-of-law is sparse. Given the state of technology and potential for the rule of law to improve, it is curious why such applicability of the

---

[163] *Algorithm Design*, TUTORIALS POINT, https://www.tutorialspoint.com/design_and_analysis_of_algorithms/design_and_analysis_of_algorithms_introduction.htm (last visited May 5, 2019).

[164] *See* Susan C. Morse, *Government-to-Robot Enforcement*. Illinois L. Rev. 1, 2 (March 19, 2018) https://ssrn.com/abstract=3143716.

[165] The first theoretical formations of computer mechanisms were envisioned by mathematician Alan Turing. His "innovation was to introduce imaginary machines that could generate computable numbers, thus converting the mathematical concept of decidability into the automated behavior of a symbol-manipulating machine that performed the repetitive operations . . . In 1950, *Mind* published his Computing Intelligence and Machinery . . .that tackled the question of whether or not machines can think." *Alan Turing*, OXFORD COMPANION TO THE HISTORY OF MODERN SCIENCE, http://www.oxfordreference.com.proxy.lib.uiowa.edu/view/10.1093/acref/9780195112290.001.0001/acref-9780195112290-e-0746.

[166] Where at least now even the American Bar Association is attuned to the need to implement more technology in legal practice as evidenced by their "Legal Technology Resource Center." *Legal Technology Resource Center*, AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/departments_offices/legal_technology_resources/ (last visited May 14, 2019). See also *Legal Technology Resource Center at American Bar Association*, AMERICAN BAR ASSOCIATION https://www.linkedin.com/in/abaltrc/ (last visited May 14, 2019) (stating that the center has existed for the last 25 years).

current technology has not been more formally introduced or examined in aiding legal decisions.[167] Instead of using scientific tools in the legal settings where science is the content of law, my aim was to convince the reader that the practice of law should function with tools that aid precision, systematic evaluation, efficiency, and fairness. The tools not only enable the formalistic ends to thrive but are robust enough to honor legal realists' objectives as well.

Elizabeth Davidson *graduated with a J.D. in May 2019 from the University of Iowa College of Law. Her first publication was with The Journal of Corporation Law as a student Note, which proposes a middle ground to cryptocurrency regulation. Elizabeth also aided in the development of the proposed ABA Resolution on Legal Ethics for AI under the Robotics Subcommittee. She worked on fintech related matters for the Commodity Futures Trading Commission (CFTC) the summer of 2018 and is sitting for the New York Bar. Elizabeth will continue work in the areas of technology, regulation, and finance.*

[167] For scientific contents of law, judges are guided by assists judges in managing cases involving complex scientific and technical evidence by describing the basic tenets of key scientific fields from which legal evidence is typically derived and by providing examples of cases in which that evidence has been used. *Reference Manual on Scientific Evidence*, FEDERAL JUDICIAL CENTER (Jan. 1, 2011) https://www.fjc.gov/content/reference-manual-scientific-evidence-third-edition-1. Conceptual frameworks for a more technical "Mechanical Jurisprudence" have been proposed and refuted with the same arguments as those against legal formalism. *See generally* Roscoe Pound, *Mechanical Jurisprudence*, 8: 8 COL. L. REV. (1908), 605-623.

The Next Big One for the Software Industry. Is Your ePrivacy Preparedness Kit Ready?

By Volha Samasiuk and Alex Gin


As we mark the one-year anniversary of the General Data Protection Regulation (the "GDPR") coming into effect, major enforcement cases with multi-million dollar fines have been largely absent.[1] *But as Helen Dixon recently noted, these cases are "not overnight."*[2] *Many investigations are still in progress, and large* fines are expected.[3] Companies with an international presence may also be tracking the numerous aftershocks in the form of omnibus privacy laws taking form outside the EU. But what comes after such a sweeping privacy regulation like the GDPR?

In a post-GDPR world, technology companies are now realizing they are stewards of their customers' data. The ability to build and maintain customer trust is becoming a critical ingredient to the reputation and success of companies that depend on data. They have more motivation than ever to meet customers' expectations not only as a compliance matter but also as a competitive advantage. Software companies can, and routinely do, collect a remarkable amount of data through their offerings and services, including user profile data, attributes about the end-user's device, crash logs, licensing and entitlement information, details about command and feature usage, communications data, authored content and related metadata. The scope of data software providers can collect from users' devices extends far beyond personal data.

For technology companies with a footprint in the EU, the ePrivacy Regulation has the potential to trigger the next big tectonic shift in how they manage collection and use of inbound data. While social media companies, advertisers and electronic communications service providers may find themselves closer to the epicenter, all technology companies that develop or leverage software may feel the impact. Based on current drafts of the ePrivacy Regulation, its material scope will cover a broader surface area than just web cookies and electronic marketing. It is still unclear exactly when the ePrivacy Regulation will be adopted and take effect. With all of the uncertainty around both the language and the timing of the regulation, it has received far less attention than GDPR. But technology

---

[1] The highest fine we have seen so far was imposed on Google LLC by the French data protection authority. The case is currently under appeal. *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC, CNIL,* available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[2] *Irish data official defends tech investigation record: 'They're not overnight', POLITICO,* available at: https://www.politico.com/story/2019/05/03/irish-data-official-defends-tech-investigation-record-theyre-not-overnight-1410541.

[3] *Dixon at Senate hearing: Fines are coming; they will be 'substantial', IAPP,* available at: https://iapp.org/news/a/dixon-at-senate-hearing-fines-are-coming-they-will-be-substantial/.

companies, in particular, shouldn't underestimate the complexity introduced by this regulation and its potential impact on software offerings and data practices.

In this article, we highlight the potential scope of the ePrivacy Regulation, its requirements for consent, and anticipated timing of the regulation. We also explore certain challenges that software companies may face in their attempts to implement the provisions of the ePrivacy Regulation, particularly focusing on on-premises or desktop application development. This article provides a starting point to help in-house counsel kick off the ePrivacy discussion in their companies, call out some key considerations, and contribute to the strategic discussions that will invariably bring in product development, data governance teams and executive leadership.

Potential scope of ePrivacy

For those companies that decide to defer efforts to comply with the ePrivacy Regulation until it is finalized or adopted, the important question to ask is whether they are compliant with the current ePrivacy Directive[4] that is already in force. The ePrivacy Directive was adopted back in 2002 and last updated in 2009 (now often referred to as the "Cookie Directive")[5]. As an EU Directive, it was implemented in national laws of EU Member States; variations in implementation led to an inconsistent legal regime and spotty enforcement across the EU. The ePrivacy Regulation, which is currently under negotiation, is poised to replace the ePrivacy Directive. Once adopted by the European Parliament and Council of the EU, the ePrivacy Regulation would apply automatically to all EU Member States, subject to any phase-in period, without the need for additional implementation in local laws.[6]

The ePrivacy Directive has already established: (a) specific rules for unsolicited communications for direct marketing purposes; and (b) a general prohibition against access to and storage of information on a user's device ("terminal equipment"), unless a user has provided consent or a narrow exception applies. The use of website cookies has attracted a lot of attention from various data protection authorities, and it remains a major focus of enforcement activities.[7] It should be noted, however, that the Directive covers any "storing of information, or gaining of access to information already stored, in

---

[4] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications),* available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

[5] *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws,* available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

[6] However, the ePrivacy Regulation, as currently drafted, will allow the EU Member States to further specify and clarify its provisions in their national laws.

[7] See, e.g., *European Union: EU regulators increase focus on cookie practices, MONDAQ,* available at: http://www.mondaq.com/unitedstates/x/791854/Data+Protection+Privacy/EU+Regulators+Increase+Focus+on+Cookie+Practices.

the terminal equipment of a subscriber or user."[8] At the same time, fines under the ePrivacy Directive are relatively low (e.g., the recent fine imposed by French CNIL was 25,000 euro)[9], but expected to escalate rapidly with the passing of the ePrivacy Regulation. It is becoming clear that ePrivacy Regulation will likely mirror the GDPR provisions on sanctions (e.g., fines up to 4% of worldwide revenue or 20 million euro whichever is greater).

At the very least, with the passing of the ePrivacy Regulation, companies may need to revisit their cookie approach to address increasing risk associated with this higher range of fines. Software companies, in particular, should also consider broadening their self-assessment to address other implementations of code capable of storing and transmitting information from end-users' devices. Examples can range from code responsible for collecting and sending telemetry about product usage, information about the terminal device itself, and metadata funneled into machine learning projects that are not necessary to provide the requested service. To address the risk of broader scope, any consent mechanism that companies implement should be flexible enough to adapt to potentially stricter ePrivacy Regulation provisions on cookies and other tracking technologies (implementation challenges discussed below).

Note also that the ePrivacy Regulation specifically aims to protect the communications of individuals as well as legal entities, and its protection, therefore, is not limited to only "personal data". This can be a challenging message to deliver to business stakeholders who have been hyper-focused on defining the bounds of personal data in order to comply with GDPR.

However, the most sweeping change presented by the proposed ePrivacy Regulation is the extension of its scope to "over-the-top" communications services.[10] Traditionally, restrictions on the use of communications content and metadata applied to telecommunications providers. However, online communications providers that offer "functionally equivalent services" such as webmail services, instant messaging services, and computer-based Voice over IP services will be brought in scope of the ePrivacy Regulation. Indeed, end users may have the same expectations of privacy and confidentiality whether they send text messages via Vodafone's network or a chat application like WhatsApp. As such, the EU bodies have argued the necessity of tackling the rapidly evolving technological landscape of the communications sector.

---

[8] *Article 5(3) of the ePrivacy Directive (as amended in 2009)*.

[9] *France: Website publisher fined for violation of the cookie requirements, DLA Piper's Global Privacy & Data Protection Resource,* available at: https://blogs.dlapiper.com/privacymatters/france-website-publisher-fined-for-violation-of-the-cookie-requirements/.

[10] Over-the-top services do not consist of conveying signals on an electronic communication network but are considered to be independent services delivered on top of the electronic communication network, see *Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, European Data Protection Board,* available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.

We should also consider the public outcry about suspect data practices and outright abuses associated with large data-driven technology companies originating mostly from the United States. If only moderate pressure builds to address it, the final draft of the regulation may not be so explicit about limiting the target area to over-the-top communication services and web-based advertising and marketing models. Leveraging the broad scope of the ePrivacy Regulation, EU data protection authorities (DPAs) would have the opportunity to cast a much wider net across the software ecosystem. Even software companies that provide communication functionality as an ancillary service (e.g., features that enable collaboration, messaging, or sharing of data or files) should closely monitor ePrivacy developments, as it potentially represents a completely new set of legal requirements for a very different scope of data compared to the coverage of the GDPR.

The current text of the draft ePrivacy Regulation does very little to differentiate between different software platforms, devices, and service delivery models. With little confidence that the final regulation (or the DPAs charged with enforcement) would provide nuanced guidance about how to implement these rules, in-house counsel and privacy professionals can serve a critical role by: (a) monitoring the posture of the regulation as it moves closer to adoption and (b) acting as translators of the regulation's text into actionable guidance and requirements for business and development teams.

Grounds for processing & secondary uses

The GDPR established a general prohibition on the processing of personal data unless such processing is based on at least one of the mandated lawful bases (e.g., consent, performance of a contract, legitimate interest, legal obligation, etc.)[11]. All of these bases represent equally valid grounds for data collection and other types of processing. In contrast, the proposed ePrivacy Regulation, similar to the current ePrivacy Directive, is focused on consent as the prevailing ground for the processing of the data in scope, namely terminal equipment information and electronic communications content and metadata, where "processing" may include the initial placement of code responsible for storing of information on the device or accessing of information, as currently described in the ePrivacy Directive.

Importantly, the European Data Protection Board (the "EDPB") insists that there should be no possibility under the ePrivacy Regulation to process electronic communications data (content and metadata) based on open-ended grounds, such as "legitimate interests" and "performance of a contract". Instead, the EDPB encourages electronic communication service providers to use

[11] *Article 6(1) of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* available at: https://gdpr-info.eu/.

anonymization techniques for further uses of such data "in order to create innovative services while preserving privacy."[12]

In brief, the ePrivacy model can be described as a broad prohibition on the processing of communications data and terminal equipment information, unless a narrow exception exists for the specific use or the software provider has found a way to secure consent. It remains to be seen whether the ePrivacy Regulation will apply to data "in transit" only or "at rest" as well. In a latter case, companies that intend to use collected data for secondary purposes (e.g., analytics, machine learning, etc.) will need to ensure that they have both (a) a lawful basis for processing under the GDPR (which may include consent or legitimate interest), and (b) consent for such secondary use (or a valid permitted use) under the ePrivacy Regulation.

Given these drastic differences in the frameworks of these two regulations, companies may want to revisit the data inventories compiled for their GDPR compliance program to prepare for the anticipated requirements of the ePrivacy Regulation. These data inventories can serve as a starting point to help identify the data in scope for the ePrivacy Directive (and, potentially, the Regulation). To augment these inventories, it may be helpful to clearly document the primary and secondary uses of data (or business purposes) and map those uses to the expressly permitted uses signaled by the latest drafts of the ePrivacy Regulation.

Software companies may also find value in conducting a broad assessment of secondary uses of data collected directly from the terminal equipment of end-users. This exercise can help establish where mitigation efforts may be needed to comply with the consent requirements of the upcoming regulation. Where companies can identify at an early stage those compliance gaps that require significant engineering and development resources, they can begin to plan for remediation of their products, services and business model while development cycles are available. This is where some strategic decisions may need to be made in anticipation of the ePrivacy Regulation.

Forecasting and preparation

The original timeline for the ePrivacy Regulation called for its effective date to coincide with the GDPR on May 25, 2018. However, competing drafts and heightened attention on the GDPR slowed down the review process among the European Commission, European Parliament, and Council of the EU (the "Council"). One year post-GDPR, the ePrivacy Regulation remains embodied in competing drafts and negotiations are still in ongoing.

At this point, the Council, under the Romanian presidency (January – June 2019), has committed to provide only a progress report.[13] There is no indication that the Council will reach a general approach

[12] *Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, European Data Protection Board,* available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.

during the current term, and any formal trilogue negotiations between the main deliberating EU bodies are unlikely to start until well after the European Parliament elections in May 2019. It remains to be seen how these elections will impact the ePrivacy negotiation process and shape the legislative priorities for the new Finnish presidency of the Council (July – December 2019) and the newly appointed European Commission whose term will start in November 2019. Accounting for all of these variables, a common draft of the ePrivacy Regulation may not be adopted by the European Parliament and Council until well into 2020.

This uncertainty may lead many U.S. companies to take a "wait-and-see" approach and further focus on their GDPR compliance efforts or put their privacy resources in some other demanding projects, such as the California Consumer Privacy Act which will go into effect on January 1, 2020. On the other hand, companies that have chosen to put the ePrivacy project aside completely may find themselves out of position to react when the regulation adopted. While the GDPR included a 24-month phase-in period for implementation, the ePrivacy drafts vary from not providing any period for phase-in to up to 24 months, creating another "unknown".

Even if parts of the ePrivacy Regulation remain moving targets, companies can start mobilizing a cross-functional team, starting with data governance, product managers and experience design specialists. First steps might include a preliminary scoping exercise of technologies and code enabling data collection from products and services, in addition to improving existing data inventories. A detailed map of data collection and uses focusing on the data in scope for ePrivacy can help companies establish the minimum amount of time needed to execute on an ePrivacy compliance project. At the very least, these exercises can help raise awareness and lay a foundation to develop a project plan to identify the triggers for further investment, deeper assessment, benchmarking, and solution design. In the meantime, companies can monitor the ePrivacy Regulation drafts[14] (though it is proved to be a tedious task) as well as policy positions pursued by the EU institutions involved in negotiations.

Implementation challenges

Software companies that determine the ePrivacy Regulation's provisions apply to their offerings and services will need to grapple with the implementation of those rules and make tradeoffs against other roadmap priorities. Providers of enterprise and professional software solutions, in particular, may face greater complexity and benefit from a longer lead time when planning for implementation. In this

---

[13] *ePrivacy: Progress report for the Council of Ministers, FEDMA,* available at: https://www.fedma.org/2019/05/eprivacy-progress-report-for-the-council-of-ministers/

[14] *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).* The recent Council's drafts of 15 February 2019 and 13 March 2019 are available at: https://www.parlament.gv.at/PAKT/EU/XXVI/EU/05/43/EU_54357/imfname_10879938.pdf (the "February Draft") and https://www.parlament.gv.at/PAKT/EU/XXVI/EU/05/76/EU_57675/imfname_10886771.pdf (the "March Draft").

section, we examine constraints often associated with software providers of installed software or on-premises solutions to help us illustrate some of these challenges.

Consider complex professional applications intended for installation on the customer's desktop machine or server. Even with the growth of SaaS enterprise solutions over the past decade, there will always be a need for on-premises software or software installed on the end-user's device or server. Large companies and government customers have strict security requirements and often require installation on their infrastructure. And for some businesses the risk of disruption to key business functions may be too high to rely upon a SaaS model for delivery of services. Without a web front-end or primary functionality that resembles a communication service, they may hope to avoid the scope of the ePrivacy Regulation. But many of these applications are still cloud-connected and very capable of facilitating collection of data from customers' devices and servers to facilitate licensing checks, enable piracy detection, deliver usage data for product improvement, report on stability issues or crashes, and drive customer persona development, to name a few examples.

Development cycle

Software companies will need to internalize with new requirements imposed by the upcoming ePrivacy Regulation as early as possible. Regardless of whether they follow a waterfall or agile development methodology, software development can take time. A major release of a complex professional application might be a year or more in the making, with code locked in months in advance of release. For long product development and release cycles, the phase-in period for the ePrivacy Regulation will be a crucial reference point.[15] Even if the regulation does not ultimately prescribe privacy settings,[16] any changes to the user interface or code responsible for storing or transmitting communication data or terminal equipment information would call for a significant engineering effort. Companies will need to work backwards from the effective date of the regulation and consider time for testing, QA, other competing priorities on product roadmaps, corresponding changes to systems responsible for storage and processing of data, and legal review. They should also build in additional time if product teams are structured in a way that creates dependencies on multiple development teams, especially in an environment that prioritizes sharing of common components across the product portfolio.

Legacy software

The Council's drafts have been largely silent on the treatment of legacy installed software, i.e., software code installed on computers or servers prior to the effective date of the ePrivacy

[15] Article 29(2) of the February Draft provides that the ePrivacy Regulation will apply from 24 months from the date of entry into force of this Regulation.

[16] Article 10 ("Privacy settings") has been deleted from the text of the Regulation by the Austrian Presidency. *JD – Proposal for a Regulation on privacy and electronic communications, European Parliament,* available at: http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform.

Regulation.[17] Products that were shipped and hard-coded to send communication data or device information cannot be easily modified after the fact (in contrast with a SaaS model). Under ideal conditions, software developers may be able to create an update to bring the installed product in compliance with new requirements. But unless the application previously included a mechanism enabling automatic updates, there are no guarantees the update would be adopted in significant numbers. Many B2B customers prohibit automatic updates. Furthermore, companies would have to navigate laws that impose restrictions around automatic download or installation of software code without end-user permission. And even if updates were viewed as a viable mechanism to address non-compliant legacy releases, how far back is reasonable? Would developers be expected to create updates for unsupported versions or applications running on obsolete operating systems and hardware?

Thoughtful consent framework

As previously discussed, the draft ePrivacy Regulation relies heavily upon consent as grounds for placing code that communicates data for certain uses. While the standard for "consent" is defined in the GDPR, concepts like "legitimate interest" and "performance of a contract" (lawful bases under the GDPR) have not found their way into the drafts of the ePrivacy Regulation. Unless the transmission of certain data is necessary for the provision of the requested service, or a narrow exception applies (e.g., fraud detection, maintaining security, etc.), developers and experience designers will have to engineer ways to capture consent to use data, for example, for internal analytics or direct marketing. If the regulation continues to insist upon collection of consent from both the end-user as well as the legal entity, developers will need to think about how to capture end-user preferences in a way that minimizes "consent fatigue" and disruption to the user experience, installation process, and deployment workflow. Even if the consent is documented in terms of service (presumably establishing assent by the legal entity), the application may still need to present an opt-in consent to the end-user. How will developers of enterprise software solutions avoid a situation where the preferences of an individual employee conflict with the preference set by their IT department?

Multiple offerings & multi-platform

While not always the case, many software companies offer a portfolio of products and services. Some offerings may follow consistent design patterns, especially if there exists some level of interoperability between applications. Others may intentionally diverge from the rest of the portfolio, presenting a unique look and feel or embodying a distinct brand. Offerings brought together by acquisition or merger can be integrated over time or intentionally left chart their independent paths. While some

[17] However, Article 10 (currently deleted from the text of the Regulation) stated that its provisions shall not apply to software that is no longer supported at the time of entry into application of the Regulation.

drafts of the ePrivacy Regulation have prescribed "user-friendly privacy settings"[18], it does not solve the issue of whether end-user consent should take a product-specific approach or be applied consistently across the portfolio. Experience designers need to think about whether the front end of their consent framework resides within each product and whether there is consistency among the different product experiences, in terms of segmentation of data, description of uses, granularity of control, and visual elements. Another option might be to centralize all consents and privacy settings in one location like a web interface that is accessible from all offerings. An inherent tension exists between a simplified user experience and the notion of providing fine granular control to end-users, especially when multiple products collect similar categories of data. Product teams will need to work closely with legal counsel to strike the right balance. Teams may also disagree about the priority of different uses of data or how to articulate these activities to end-users. They should expect to collaborate across product team boundaries to solve for ePrivacy requirements, even if they are only integrating a common component. In all cases, it will be important to build a framework that is flexible enough to adapt to changing legal requirements, customer expectations and uses of data.

A multi-platform portfolio presents similar challenges as above. The instrumentation technologies may vary widely from a desktop application to a mobile app, even though the title of the applications may be identical. For a single mobile app, the tools, systems, and data flows may be unique to each mobile operating system (i.e., Android versus iOS). Users' expectations about what data is collected through different devices may also be an important factor. Just as one wouldn't expect identical functionality between a professional desktop application and a light-weight mobile app, consents and privacy settings will need to be tailored to how users expect to interact with a particular platform or device. How should we respond if an end-user permits use of data transmitted from their desktop machine, but opts-out of the same use on their mobile device? Should we assume that their most recent choices relate to all devices, platforms, and products and propagate preferences accordingly? Or do we allow for differentiation and granular control based on the above factors, and come up with policies to reconcile contradictions, all without leaving end-users in a state confusion? For technology companies that face some of these challenges, their in-house lawyers may want to start raising these questions with key stakeholders for product development and experience design.

Conclusion

As the ePrivacy Regulation gets mired in negotiations, it may be easier to hope that it never arrives or that its target area remains specific and out of range. But our failure to track its potential impact on the software industry and to consider the challenges of implementing a solution would a lost opportunity to prepare for the inevitable. With the spotlight on data privacy, proactive steps to build trust and address customers' concerns over the range of data shared by their devices can be a strong competitive differentiator.

---

[18] *Recital 20a of the February Draft*, available at: https://www.parlament.gv.at/PAKT/EU/XXVI/EU/05/43/EU_54357/imfname_10879938.pdf.

We summarize the above discussion with the following points:

- The ePrivacy Regulation will undergo numerous changes before adoption, and we have no guarantees about the timing of adoption or the length of any phase-in period.

- The scope of data covered by the ePrivacy Regulation is much broader than "personal data". We do not know whether regulators will interpret the scope liberally or focus on marketing and cookies. However, the Regulation will give regulators the powerful tools to examine other technologies besides cookies.

- The ePrivacy Regulation heavily leverages consent as grounds for processing data as well as a handful of narrow exceptions for permitted uses of certain data. Legitimate interest and other lawful bases under the GDPR are not available, suggesting that processing of personal data may be treated inconsistently under the two regulations.

- The ePrivacy Regulation demands tracking of a broader set of data attributes, as well as primary and secondary uses. This exercise becomes increasingly challenging as companies apply data science and bring machine learning models to bear on existing data sets, exposing the limitations of consent as a basis for processing.

- Software companies offering more than one product or delivering a multi-platform offering have a challenging road ahead and need to start taking stock of their data collection practices, including notices and consents surrounding their product experiences.

Due to the uncertainty of the status and language of the regulation, most companies are waiting for further direction. But they can take some preliminary steps now to increase their state of readiness for ePrivacy. This includes building cross-functional teams, updating data inventories, documenting uses, and planning a coherent strategy for consent.

And if the ePrivacy Regulation stagnates and never materializes? At least you will have run through the drills and put your company in a stronger position to respond to the next inevitable big data privacy development. As pressure on politicians and governments continues to build in this post-GDPR era, it is just a matter of when and where the next data protection law or regulation will strike.

Alex Gin *is the lead Data and Analytics Counsel at Autodesk, where he supports and enables the company's centralized data and analytics organization to develop data-driven insights for business teams and customers. He focuses on data governance, analytics programs and platforms, machine learning and product development. Alex previously worked in the Technology Transactions Group of Morrison & Foerster LLP, based in San Francisco.*

Volha Samasiuk *is Privacy Counsel at Autodesk, where she helps business teams to navigate evolving legal and regulatory landscape around privacy and data protection and ensure that the company uses*

customer data responsibly. Trained in civil and common law, Volha previously worked as Senior Counsel and Privacy & Compliance Officer at Wargaming, an international video game company, based in its Belarus, Cyprus, and U.S. offices.

An Analysis of the Legal Framework of e-Commerce in India

By Arunabh Choudhary and Tanvi Muraleedharan


In the last decade, India underwent a digitization revolution, there was a phenomenal shift that was felt in the market as India went online. According to Morgan Stanley the growth is driven by a combination of rising internet penetration, with high digital literacy in India and drop in data access costs and flow of credit to consumers and small and micro enterprises.[1] Despite the wide user base spread across tier 1, tier 2 and tier 3 of Indian cities, India still does not have an exhaustive regulatory framework dealing with e-Commerce. However, India does have certain restrictions and compliances placed on e-Commerce companies, especially in relation to foreign direct investment. The regulations on e-Commerce were more from restricting and regulating foreign companies to enter into India.

(I) Extant regulatory framework dealing with e-Commerce in India:

1) Forex Regulations:

Typically, e-Commerce entity is governed by the rules and regulations governing the business of the entity. If for example the entity is an online clothing store, all compliances and legal requirements applicable to a physical clothing store (due to the nature of business) should not apply to the online entity as the same only be engaged in selling of clothing items and not manufacturing it. In the event such online entity intends to do telemarketing for its products, they will be required to procure a telemarketing license like any other business. This we believe would still be a reality even after a specific regulation for e-Commerce is brought into effect. However there has to be differentiation of regulation of e-Commerce entity given they may not be involved in many of the products.

There are however certain specific requirements and regulations which impacts an e-Commerce business and the same is usually dependent on the type of business model that the e-Commerce business is based on.

Usually an e-Commerce entity follows either a marketplace model or an inventory-based model. In case of a marketplace model, the e-Commerce business would be providing a platform for all the sellers and buyers to meet and would essentially be acting as an aggregator. The perfect example for the same is Amazon. The inventory-based model is where the e-Commerce business will own and trade its inventory.

---

[1] Morgan Stanley. (2017). India's Digital Future. [online] Available at: https://www.morganstanley.com/ideas/digital-india [Accessed 10 May 2019].

This distinction is very crucial as most of these e-Commerce players (at least the bigger players) are massively funded by offshore investors. Per the Indian foreign exchange regulations, infusion of foreign funds into an inventory-based model e-Commerce platform will require the prior permission of Reserve bank of India (**"RBI"**), the central bank of India, which is seen as doing retail activity in India.[2] Only marketplace model platforms are allowed infusion of foreign funds, without any prior approval (except sectoral approvals). Further, a recent notification of the Department for Promotion of Industry and Internal Trade (**"DPIIT"**), which came into effect on 1st February 2019 (**"Notification"**), clarified the manner of confirming whether an entity is following inventory-based model or not. The Notification states that:

(a) The e-Commerce entity will be considered using an inventory-based model if:

(i) the e-commerce entity exercises ownership or control over the inventory. Exercising control in this instance means if more than 25% of the inventory of a single vendor is purchased by the e-Commerce platform or its group companies; or

(ii) an entity in which e-commerce entity or its group companies holds equity shares sell its products on the platform run by such entity; or

(iii) it directly or indirectly, influence the sale price of any goods or services and fails to maintain a level playing field. In case services provided by connected entities then that should be treated as per arms length mechanism; or

(iv) it mandates any seller to sell any of their product exclusively on its platform.

(b) Every marketplace entity is required to confirm compliance with the Notification by 30th September of every year.

(c) Marketplace model requires the entity to provide the name, address, and other contact details of the seller of the product. Post sales, delivery of goods to customers and the customer satisfaction will be the responsibility of the seller.

These changes have impacted a lot of the major e-Commerce players as most of them were trading from vendors which are controlled by them. Further, e-Commerce companies, will be restricted from procuring customers with deep discounts and exclusive offerings. These changes were effectively made to ensure that the offshore funded e-Commerce platforms will not be anti-competitive and to create a level-playing field for home-grown platforms.

[2] RBI notified vide notification no. FEMA.387/2017-RB dated 9th March, 2017.

2) Taxation Laws:

Foreign e-Commerce entities conducting business or where its websites/ apps are made available to persons in India (even though there is no physical presence in India) may be subject to taxation of their profits in India as a result of a recent addition to the Income Tax Act, 1961 in relation to 'significant economic presence'[3]. The concept of significant economic presence gets triggered under two circumstances (i) if payments arising from India in relation to transaction in respect to any goods, services, or property carried out by any foreign person including any facility provided by the non-resident for download of any data or software in India crosses certain thresholds[4] or (ii) if there is a systematic and continuous soliciting of the consumers through digital means or if there is interaction with such number of users through digital means.

(II) Draft National e-Commerce Policy:

The lack of a clear regulation is one of the crucial concerns that a foreign entity has in relation to starting a business in India. Hence, in an effort to provide a comprehensive e-Commerce policy, the DPIIT introduced the Draft National e-Commerce Policy on 23rd February 2019 (**"Draft Policy"**). The Draft Policy places significant emphasis on the regulation of foreign e-commerce website and apps (**"Foreign E-com"**), data localization and creation of a level playing field for domestic e-Commerce players.

1) **Registration Requirements:** Draft Policy has introduced certain fresh compliances for Foreign E-coms. One significant change in this regard is that the Draft Policy proposes that every e-Commerce entity which transacts in India must have a registered business entity in India. This would effectively mean that for any Foreign E-com platform accessible in India would require to be (i) registered in India and (ii) an individual will not be able to operate a Foreign E-com website in India. We believe that DPIIT should relax this requirement. Considering that not every e-Commerce platform transacts with Indian consumers on a regular basis, Foreign E-coms conducting sporadic and irregular transactions may be exempted from this requirement. Furthermore, considering even foreign exchange laws of India allows for Indian residents to carry out current account transactions, outside India, within the limit of USD 2,50,000 per annum and that IT laws prescribes for thresholds in case significant economic presence, a threshold can be brought in here.

2) **Taxation:** It is clarified in the Draft Policy that in the event Foreign E-com company has 'significant economic presence' in India, the company may be taxed in India.

[3] Section 9(1)(i) of the Income-tax Act, 1961
[4] These thresholds are yet to be notified.

3) **Data Offshoring:** Considering that one of the most valuable assets of an e-Commerce company would be the data of its consumers, the entity with the ability to amass the maximum data will gain a great advantage over its competition. Without access to adequate data, MSMEs and start-ups remain at a disadvantage to develop a large number of innovative solutions.

To remedy this imbalance in competition and considering that the data of Indian citizen should continue to be property of the sovereign and the citizen, the Draft Policy has recommended localization of data. This is not the first effort by the government towards data localization. The RBI, in 2018 had started the movement towards data localization in India, by mandating for all Indian users' financial data to be stored in India. Further, the Personal Data Protection Bill, 2018 ("**PDP Bill**") passed by the Lok Sabha also recommends that certain personally identifiable information be stored within the territorial limits of India.

The Draft Policy in harmony with the PDP Bill makes strong proposals towards data localization and restricting cross-border flow of data. However, the Draft Policy is not clear on definition of data and the nature of the data which needs to be localized. One of the suggestions to DPIIT on the Draft Policy is that there should be an unambiguous definition of data and a comprehensive list of information (or type of information) that is restricted from cross-border transfer. The requirement to store even the most mundane information in India is highly restrictive and excessive.

It is further required that the data stored outside India be restricted from being accessed by the government authorities (of the place where it is stored). We believe that this may be practically difficult to carry out for the entity that is registered in such jurisdiction and the same may be eventually made part of an inter-governmental treaty rather than a requirement on a Foreign E-com.

4) **Infrastructure support:** Considering that the data storage infrastructure of India will not support the data localization requirements stated in the Draft Policy, a period of 3 years is provided to the stakeholders to build up the necessary infrastructure and may also be granted an infrastructure status. Between the Draft Policy and PDP Bill, we see setting up of data centers in India as a great opportunity. Further, domestic alternatives for cloud services and email facilities will be promoted.

5) **Anti-counterfeiting and Anti-piracy measures:** The Draft Policy states that the government will also be enforcing stringent anti-counterfeiting and anti-piracy measures, to be undertaken by the e-Commerce players. Some of these requirements include:

   (a) the seller to undertake the authenticity and genuineness of the product and make these declarations available to the consumers;

(b) the e-commerce platform to provide trademark owners an option to register themselves and after such registration the e-commerce platform should intimate the trademark owner anytime any product using the trademark is sold on that platform;

(c) blacklist sellers found to be selling counterfeit products and remove or disable access to copyright infringing content; and

(d) mechanism is envisaged to be created so as to alert the brand-owners and the copyright owners if a counterfeit or pirated product is being sold.

These mechanisms and undertakings will have to be built in the agreements with the vendors/sellers by the Foreign E-coms. One of the crucial issues that has come to the forefront is that the Draft Policy allows the e-Commerce businesses to adjudicate the matters relating to intellectual property infringement of any person and take actions against such infringing seller. This approach by the Draft Policy goes against the judgement of the Supreme Court in the Shreya Singhal case[5], which states that the intermediaries are neither competent nor do they have proper jurisdiction to adjudicate matters related to infringement of intellectual property.

The present laws, dealing with the liability of intermediaries has provided certain protection to the intermediaries. It protects intermediaries like social media companies, e-commerce sites, etc. from liability for any content they host.[6] Intermediaries are obligated to exercise due diligence for the content uploaded and must take down illegal content within 36 hours on receiving a court direction or government order to do so. However, the changes as proposed in the Draft Policy would extend the liability of the e-Commerce and they would no longer merely act as an intermediary.

6) **Consumer Protection Mechanism:** One of the proposals made in the Draft Policy is that there needs to be a transparency and non-discrimination in publishing of ratings and review and require the e-Commerce websites to fish out any fake and ingenuine ratings. However, it is extremely difficult for e-Commerce websites to track and authenticate every review. Hence, we believe that the final e-Commerce policy may set out parameters for verification of ratings and reviews for the e-Commerce websites and the e-Commerce entities may be required to maintain records furnishing the compliance with the same.

Further, the e-Commerce entities are required to set up a grievance redressal mechanism in a time-bound fashion. The government is even considering moving towards an electronic redressal mechanism.

[5] Shreya Singhal v Union of India, 1 SCC 5 (2015).
[6] Section 79 of Information and Technology Act, 2000.

7) **Other Key Aspects:** Several steps have been undertaken under the Draft Policy to increase the accountability of the sellers as governance and supervision over these entities. Some of these measures are provided below:

   (a) Access to Indian consumers will be restricted to non-compliant websites. This access will be restricted by the relevant governmental body;

   (b) All offshore shipments are required to be channelized through the customs route; and

   (c) With the exception of life-saving drugs, the shipment of products through 'gifting route' will be completely banned.

Conclusion

With the rapid growth of India as a consumer state, the requirement for a specific law governing e-Commerce cannot be denied. However, there is also a sense from the Draft Policy that it is trying to curb competition faced by the domestic players along with regulating the e-Commerce entities. The Draft Policy is in its infancy currently, and it will be upon the stakeholders and the government how they would want to shape up the e-Commerce sector of India. We believe that a balance will be struck between inviting more foreign investments in the e-Commerce sector and promoting domestic players.

The Draft Policy has covered quite a myriad of issues relating to regulating, promoting e-Commerce industry and in protecting the consumers. However, an approach has to be adopted by the Government in further developing the Draft Policy in a manner that it does not isolate India from the international market. Further, the policy may need to be more forward thinking to cover for newly emerging technologies and paradigms on electronic commerce, including IoT, blockchain and artificial intelligence and be balanced in its approach.

*Mr. **Arunabh Choudhary** is a partner in Juris Corp and has work experience of 10 years. Arunabh advises many new edge tech companies. (email: arunabh.choudhary@jclex.com)*

*Ms. **Tanvi Muraleedharan** is a senior associate and is part of Tech team. Tanvi has been advising various Tech companies. (email: tanvi.muraleedharan@jclex.com)*

Overview: Brazil's New Data Privacy Law

By Renato Opice Blum and Camila Rioja Arantes

The Brazilian House of Representatives approved the Brazilian data protection draft bill (PL 53/2018, "LGPD") on May 29, 2018. Following subsequent passage by the Federal Senate, the LGPD was signed into law by former President Temer on August 14, 2018[1]*. On December 27, 2018, the Provisional Measure* no. 869/2018 was published in the Official Gazette, amending the LGPD and creating the National Data Protection Authority. The law is an important landmark in Brazilian history and draws inspiration from the European General Data Protection Regulation ("GDPR").

The law will enter into effect in August 2020. It may seem like a long time from now, however, considering all that needs to be done before the law goes fully into effect, it is actually a limited time-frame[2]. As a bit of a background, Brazil's very first legislation concerning the Internet, the Law 12,965 from 2014[3], best known as "Internet Civil Landmark", is quite recent and underwent a lot of criticism. The Brazilian Constitution[4], the Consumers' Code (Law 8.078/1990)[5] and the Information Access Law (Law 12.527/2011)[6] have also been used to support data-related claims.

As regards the "Brazilian GDPR", the draft bill origins date back to 2009, when first drafted within the Brazilian Ministry of Justice and after a procedure that involved intense debates and public consultations. The final wording of PL 53/2018 is also the result of other bills that were under analysis by the chamber of deputies, PL 4060/2012 and PL 5276/2016. It is worth clarifying that a second draft bill concerning data privacy was also under discussion in the Senate (PLS 330/2013)[7] concomitantly. Both projects, the Chamber of Deputies and the Senate one, were facing delays in the processing

---

[1] Approval was accompanied by partial vetoes to the creation of the National Data Protection Authority, some provisions on data processing by public authorities and some penalties for infringement of the law - such as suspension of operations of the offender's database.

[2] In Europe, for example, where data protection regulations were already in place, companies also had 2 years to adjust to the new regulations (GDPR), which in many cases proved not enough. The aforementioned Provisional Measure Extended the *vacatio legis* of the legislation, previously stablished in 18 (eighteen) months.

[3] For the Internet Civil Landmark bill (Portuguese only) please refer to http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (last visited May 10, 2018).

[4] For the Brazilian Constitution (Portuguese only) please refer to http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (last visited June 20, 2018).

[5] For the Consumers' Code (Portuguese only) please refer to http://www.planalto.gov.br/ccivil_03/Leis/l8078.htm (last visited June 20, 2018).

[6] For the Information Access Law (Portuguese only) please refer to http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (last visited June 20, 2018).

[7] As a last remark on the legislative process, the Reporting Senator will have the option to fuse the wording of the PL 53/2018, with the PLS 330/2013. This would cause the amended text to revert to the Chamber of Deputies, and ultimately lead to a delay in the approval process, thus inflate further debates.

mainly due to the Brazilian political scenario but were pushed forwarded by two main events: the Cambridge Analytica scandal and the GDPR, that came into force May 25, 2018.

LGPD applies to the processing (including operations such as collection, use, storage, transmission and erasure) of personal data (any information relating to an identified or identifiable natural person, including but not limited to name, national identification numbers, location data and interests) that takes place in Brazil or relates to data subjects who are in the country, even if conducted by individuals or enterprises located abroad. Materially, the LGPD will apply to anyone – whether a person or legal entity, governed by public or private law who processes data, including digitally.

The provisions explained above stress that that the LGDP has extraterritorial reach. All companies that process Brazilian data will be subject to its provisions, despite having or not an establishment in Brazil. Another important provision addresses cross-border data transfers, which will be made easier with countries that meet adequate data protection standards. The law includes principles which should guide processing, including: lawfulness; purpose limitation; data minimization; transparency; non-discrimination; safety; damage control; responsibility and accountability; free access; and data accuracy. Also, security by design, data portability, the drafting of personal data protection impact reports, and the presence of a data protection office are examples of a new reality controllers will have to face when the legislation goes into full effect.

In this regard, it is important to mention that international personal data transfer is possible under specific rules. For instance, when appropriate safeguards are in place (e.g. data protection clauses, binding corporate rules, standard contractual clauses, certification mechanisms), or if authorized by the National Data Protection Authority. Other possibilities include: (i) international legal cooperation for investigation purposes; (ii) to protect life; (iii) to countries offering adequate levels of data protection and (v) if the subject has given specific consent.

Due to the legislation, users' rights rise, given the emphasis on the right of access (i.e., data subjects can request access to all personal information held by controllers), which entails the right of rectification and updating of information. Although children's data already finds protection in specific child-related legislation, stricter provisions will apply under the "Brazilian GDPR". Several industries will be affected by such provisions, including banks, and the government itself. The impact of the legislation will be felt vividly in the daily activities with those active in IT and software development, compliance, human resources, information security, IT and marketing, among others. In a nutshell, the rights of data subjects under LGPD are:

- confirmation of processing activity;
- access to their data;
- correction of incomplete data;

- pseudonymization, blocking or erasure of unnecessary, excessive or illegally processed data;
- erasure of personal data;
- portability of their data to other service or products providers;
- information about entities which had access to their data;
- information about the possibilities of refusing content;
- revocation of consent;
- complain to the National Data Protection Authority;
- opposition to processing, if irregular.

It should be noted that *sensitive personal data* from the data subject faces a higher level of protection, as it encompasses: (i) filiation to religious, philosophical, political and labor organizations; (ii) racial or ethnic origin; (iii) political opinion; (iv) data related to health and sexual life; (v) genetic or biometric data. In this regard, it should be noted that the LGPD does not allow for sensitive personal data to be used for the purposes of redirecting advertisement. The legislation provides legal grounds for processing sensitive data, that include: (i) specific and clear consent; (ii) health protection[8]; (iii) fraud prevention and subject safety; (iv) studies by research organizations; (v) execution of public policies, protection of life; (vi) regular exercise of rights and (vii) compliance with law and regulation.

As regards pecuniary fines, these may reach as high as 2% (two percent) of the total revenues earned by the company, economic group or conglomerate in Brazil in the fiscal year preceding the commencement of an investigation, excluding taxes, but limited by a cap of BRL 50 million per infringement (roughly USD 13 million). Other applicable sanctions encompass:

- the erasure of personal data;
- blocking of processing;
- notices;

[8] The Brazilian health market is very relevant to the economy. Thus, any legislation affecting such area is of interest to the industry in general, as it may generate new and relevant opportunities for doing business in the country. As regards the relevant of the health market in Brazil it is worth quoting an excerpt of a recent article by Crowell Moring, "*Brazil's healthcare market is one of the most important in Latin America, with the largest population in the region of over 200 million and an elderly population expected to expand from 20 million to 65 million by 2050. Recent estimates place the value of the Brazilian digital health market at over US $843 million.*" Available at https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Beat-by-Beat-Latin-America-Is-Headed-Toward-a-Digital-Health-Transformation .

- publication of the offence.

It should be noted that the National Data Protection Authority will consider different aspects when deciding applicable sanctions. Recidivism, good faith, financial aspects and the advantage obtained in the case, extent and seriousness of damage and cooperation with the authority are key factors that will influence and impact fine imposition. Internal procedures, governance and best practices adopted will also be noted.

In summary, some of the main points encompassed by LGPD are outlined below:

- Scope:

It applies to any activity that involves the use of personal data - including the ones carried out by internet. Examples include employment data and relationship with consumers.

- Extraterritorial Scope:

The legislation applies to companies located outside Brazilian territory, despite any local presence in the country. It has broad applicability – even broader than GDPR. To further clarify the matter, we highlight some circumstances that are irrelevant for assessing the extraterritorial applicability of LGPD: (i) the media in which data is processed; (ii) companies' headquarter location; (iii) data storage locations and (iv) data subject's' nationality;

- Lawful Basis for Processing:

Consent is one of the hypotheses provided that is able to legitimate the processing of personal data. Other hypothesis also includes the need to fulfill legitimate interests of the controller and contractual need;

- Key Principles:

Lawfulness; purpose limitation; data minimization; transparency; non-discrimination; safety; damage control; responsibility and accountability; free access and data accuracy;

- Data Subject Rights:

Among others, right to information, access, data portability, erasure, amendment and revocation of consent;

- Specific Rules:

Apply to the processing of sensitive data, children and teenager data and international data transfers;

- Data Mapping:

Data Processing activities shall be recorded in a specific report.

- Data Protection Officer (DPO):

Every company acting as a controller must designate a DPO. Still subject to debate, the new wording provided by the Provisional Measure no. 869/2018 apparently dismissed the need for the DPO to be a natural person. The DPO is responsible for receiving and responding to data subjects' requests, interacting with the National Data Protection Authority and providing guidance for both employees and contractors about data protection practices;

- Notification:

Mandatory in some cases, including data breaches in given situations;

- National Data Protection Authority:

The Authority has technical autonomy, and is responsible for ensuring the protection of personal data, editing rules and procedures related to the protection of personal data, requesting information from data controllers and operators, besides supervising and applying sanctions;

- Automated decisions

The Provisional Measure no. 869/2018 amended the LGPD in this regard. Decisions solely based on automated processing of personal data were previously subject to review by a natural person as a right of the data subject. The new wording, however, scratched "*natural personal*" from the text, which means the whole process – decision and review – may be done in an automated fashion.

The main goal of the law is to empower the individual with ownership and control of his own data, besides setting accountability for the processing of data, and the provisions outlined above set forth a coherent framework for achieving this outcome. Assuring rights to users and preventively protecting their data is an effective measure to avoid unnecessary exposure. In addition, one way or the other, the level of accountability required of companies and the penalties set forth will fuel immediate important changes concerning safety of data in the market.

The new legislation is an important message to other countries Brazil maintains commercial relationships with, besides making business safer for international companies treating Brazilian data. Such important step may enhance business and power the data economy in Brazil. Having a clear

perspective of the limits for handling personal data allows for more security, which in turns attracts business and investors. Brazil has undergone a tough recession period, and personal data drive business are certainly a market to explore once legal limits are set and observed.

New career possibilities are also on spotlight given the legislation. Acting as a company DPO is a highly specialized role, that requires relevant knowledge in corporate governance, technology and privacy. Thus, the new requirement and role brings an opportunity for those interested in taking a step further in the data privacy and protection area and advancing their careers to a very challenging position that will require technical knowledge and creativity.

Renato Opice Blum *was a judge at the MIT Inclusive Innovation Challenge (2018). MSc, attorney and economist; Digital Law Cyberlaw and Data Protection Program Coordinator at Research and Education Institute (INSPER); Digital Law Coordinator at Sao Paulo Law School (EPD); Member of the Executive Council of the Technical Study of the Internet of Things – IoT; Former Vice-Chair of the Privacy, E-Commerce and Data Security Committee of American Bar Association (Intl. Law) and Vice-Chair at the International Technology Law Association South America Membership Committee; Member of Octopus Cybercrime Community (Council of Europe); Member of EPA's Policy and Scientific Committee – EPA'S Think Tank; EuroPrivacy Board Invited Member (Data Protection); President of Sao Paulo Lawyers Institute Standing Information and Technology Studies Commission; Coordinator of Study Commission of Digital Law of the Superior Council of Law at State Federation of Commerce (FECOMERCIO); Coordinator and co-author of the book "Manual of Electronic Law and Internet".*

Camila Rioja *was a judge at the MIT Inclusive Innovation Challenge (2018). Mentor for the "HackBrazil", an initiative lead by the Brazil Conference at Harvard & MIT. Postgraduate Diploma in Economics for Competition Law at King's College London (2015/2016). Economic Law course from the Superior School of the Brazilian Bar Association, Brasília chapter (2012). Graduated from the Centro Universitário de Brasília – UniCEUB. Admitted to the Brazilian Bar Association – OAB in the same year. Camila advises clients in matters involving digital law, new technologies, data privacy and protection. As a competition/antitrust lawyer, focuses her practice on merger filings, high profile cartels defense and other anticompetitive behaviors. Camila also concentrates her practice in compliance and anti-bribery issues, advising clients on the implementation and review of compliance programs and policies. Camila has hands-on experience in several industry segments, such as transportation, health care and agribusiness, among others.*

Another Depressing Day for U.S. Data Privacy

By Thomas Shaw

At one time, the United States was the leader in both data privacy legislation and enforcement. Unfortunately, those days are long since passed, seen clearly through the lack of a national data privacy statute that allows data subjects to always remain in control of their personal data and penalizes organizations that take this control from data subjects without their authorization. For enforcement, it is hard to remember when there last was a material penalty assessed by the FTC on one of the large data-hoarding organizations, one that really hurt them financially enough to change future behaviors and to send a message loud enough that all other organizations using the personal data of others with little or no compensation would notice enough to change their approaches and business models. While U.S. states have certainly jumped into the gap with a plethora of privacy and security laws to assist their own citizens and through enforcement actions brought by their attorneys general, the fact remains that even with the push by states, it is still the wild west of data privacy in America, as two recent federal court cases based upon state law again demonstrate.

As I demonstrated through numerous cases in U.S. federal courts discussed in Chapter 4 of *Information and Internet Law - Global Practice*, data subjects are typically unable to avail themselves of damage remedies for privacy violations because they cannot show a sufficient present and concrete injury. Courts in general have held that appropriating and disclosing without authority the personal data of others is not presently an injury, and if it is, the injury is not sufficiently concrete, despite the professional, emotional or other distress injuries that a data subject may endure. Imagine if a bad actor was to break into your house and steal all your personal records, such as your diary, your medical prescriptions, your financial statements, your intimate photos, etc. Then they were posted these online. Do you have a present and concrete injury in fact sufficient to sustain a lawsuit in federal court? Likely not, you would have to wait and see if you are truly injured by the posting, such as a monetary loss arising from the theft of your financial statements. The actual fact of the unauthorized taking and use of your personal data, does not allow you to recover through either distress damages related to knowing your most intimate information has been appropriated and disclosed or based on statutory penalties arising from each occurrence of unauthorized appropriation and disclosure.

The two recent cases both dealt with unauthorized disclosures of personal data and state privacy law, one through a data breach and one as an alleged business transaction. The business transaction involved the disclosure of student data. In *Squeri*,[1] former students of a college that had closed were suing based on the disclosure of their personal data to another educational institution. After Mount Ida College closed at the end of the academic year in 2018, the financial and academic profiles of the students were transferred to the University of Massachusetts (UMass) without the knowledge or

[1] Squeri v. Mount Ida College, No. 1:18-cv-12438 (D. Mass. May 2019).

consent of the students. Among other claims, the students asserted a breach of privacy under state law when their data was transferred to UMass Dartmouth to ensure they were all automatically enrolled in that institution for the coming school year. The court pointed out another difficulty with American educational privacy laws in that the students could not assert a claim under FERPA, due to the lack of a private right of action. It then looked to the requirements for a privacy violation under state law, that the invasion of privacy must be unreasonable and substantial or serious. Quoting from a case 35 years prior, the court noted that "legitimate countervailing business interests . . . may render the disclosure of personal information reasonable and not actionable under the statute."

The court ruled that the transfer was done for a legitimate business reason, to enroll the students in a successor academic institution. Then, focusing on the security of the transfer, it noted that the transfer was done using anonymized unique student identifiers, under the guidance of the office of the state's attorney general. The court quoted from prior cases that said because the transaction was allowed under state law, the "the invasions of privacy associated with its taking place were 'justified" and that "The statute obviously was not intended to prohibit serious or substantial interferences which are reasonable or justified." There was no mention in the ruling about the data subjects' rights of prior notification or the right of consent before disclosure to third parties, let alone the right to prohibit such transfers based on the types of personal data to be disclosed.

In *SuperValu*,[2] the plaintiffs were suing over two data breaches initiated by hackers at a series of retail outlets in 2014. The hackers stole "customers' card information, including their names, credit or debit card account numbers, expiration dates, personal identification numbers, and card verification value codes." The original complaints had been dismissed due a lack of standing for no present injury, as the information acquired was not sufficient to initiate identity theft, so the injury was merely speculative. One complaint was not dismissed, as a plaintiff in Illinois had demonstrated a fraudulent charge to his account after the data breaches. This plaintiff brought forward four types of claims under state law: negligence, consumer protection, implied contract, and unjust enrichment. The circuit court of appeals reviewed the claims and found that each failed to state an adequate basis for relief.

Negligence requires a duty of care, a breach of the duty, and a proximate injury from that breach. The plaintiff asserted that the retailer owed a duty of care to protect his credit card details from cyberattacks. The federal circuit court said that under state law "there is no affirmative duty to protect another from a criminal attack unless one of four historically recognized special relationships exists between the parties." Because the state supreme court had not yet ruled on whether there was such a special relationship between customer and retailer in regard to protecting data from cyberattack, the circuit court predicted what the state supreme court might do, by looking at a single state court of appeals decision, which "appears to hold that the state does not recognize a duty in tort to safeguard sensitive personal information." From that, the circuit court dismissed the negligence claim.

[2] In re: SuperValu, Inc. Customer Data Security Breach Litigation, No. 18-1648 (8th Cir. May 2019).

The plaintiff then looked to the FTC Act and the FTC's role in privacy and security rulings as creating a duty of care for consumers and a right of action as allowed under state law. The court said this required that plaintiff be a member of the class to be protected, that the right of action is consistent with the purpose of the statute, the plaintiff's injury is one the statute is meant to protect, and that the right of action is necessary to provide a remedy. But then it ruled that the FTC was alone appointed to redress such privacy claims and that there was nothing to suggest that the FTC was failing in its mission. It ruled the evidence proffered was not sufficient to pursue the negligence claim on this basis.

The court then reviewed the consumer fraud claim but dismissed them with the too familiar reasoning used by federal courts: "Holmes's alleged injuries—the expenditure of time monitoring his account, the single fraudulent charge to his credit card, and the effort expended replacing his card—do not constitute actual damage. The time Holmes spent protecting himself against the threat of future identity theft does not amount to an out-of-pocket loss. We previously held that the risk of future identity theft was too speculative to create standing in this case." It also said that his pecuniary loss, the fraudulent charge on his credit card, may have been reimbursed by his credit card company and he could not use the collateral source doctrine (e.g., being reimbursed for injuries through insurance) as the credit card company who potentially reimbursed him was not wholly independent of the tortfeasor.

The court could not find an implied contract between the retailer and the consumer. For unjust enrichment, the plaintiff alleged the retailer obtained his monies from shopping purchases made after the first data breach, because of untimely notice to consumers of the breach. It was alleged he would not have shopped there if he had known of the breach. The court noted that "He did not pay a premium for a side order of data security and protection." Because there was no allegation that a specific portion of his payments to the store for groceries went for data protection, he did not show that there was a "benefit conferred in exchange for protection of his personal information nor has he shown how SuperValu's retention of his payment would be inequitable." The court therefore found no basis for unjust enrichment. The court of appeal's rulings will make it difficult, at least in this federal circuit, for data breach victims to succeed in obtaining damages after the unauthorized use of their personal data.

Thomas J. Shaw *runs DPO Services from the EU, is the author of the* DPO Handbook – Data Protection Officers under the GDPR, Second edition *and numerous other legal technology, privacy, and history books, and is the editor/founder of this publication.*