FIU Law Review

Volume 17
Number 2 *Privacy Discussion Forum – University of Stockholm (Stockholm, Sweden, 2022)*

Article 7

Spring 2023

The Need for Curtains of the Soul: Privacy Versus Transparency in the Instrumented World of Algorithmic Artificial Intelligence

Michael Martin Losavio
Department of Criminal Justice University of Louisville, michael.losavio@louisville.edu

Online ISSN: 2643-7759

Recommended Citation

Michael M. Losavio, *The Need for Curtains of the Soul: Privacy Versus Transparency in the Instrumented World of Algorithmic Artificial Intelligence*, 17 FIU L. Rev. 309 (2023).
DOI: https://dx.doi.org/10.25148/lawrev.17.2.7

THE NEED FOR CURTAINS OF THE SOUL: PRIVACY VERSUS TRANSPARENCY IN AN INSTRUMENTED WORLD OF ALGORITHMIC ARTIFICIAL INTELLIGENCE

Michael M. Losavio[*]

ABSTRACT

> After the decisions denying the distinction attempted to be made between those literary productions which it was intended to publish and those which it was not, all considerations of the amount of labor involved, the degree of deliberation, the value of the product, and the intention of publishing must be abandoned, and no basis is discerned upon which the right to restrain publication and reproduction of such so-called literary and artistic works can be rested, *except the right to privacy, as a part of the more general right to the immunity of the person,—the right to one's personality*.[1]

We approach a privacy singularity in pervasive data collection and inference that may reveal all about our lives. While privacy might not yet be dead, we struggle to maintain its shield for personal autonomy. Part of this contemporary challenge comes from the massive data sets generated every day everywhere. And then the powerful analytics that reveal all. This is further challenged by efforts at data transparency that may reveal too much of one's life. Preservation of privacy, if we deem it important enough to preserve, must have a robust set of technical and legislative implementations on collection, storage, transmission, and use of all such collections of data, public and private.[2] This includes regulation of governmental and private transparency to best assure the protections of the privacy of people. But such protections may conflict with laws protecting freedom of expression or supporting law enforcement, making for greater justification for regulation that demonstrates a compelling need to protect the lives and personal

[*] Associate Professor, Department of Criminal Justice and Department of Computer Science and Engineering, University of Louisville.

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 207 (1890) (emphasis added).

[2] These are some of the issues that were discussed at the 2022 Privacy Discussion Forum in Stockholm, Sweden, as described by Professor Russell L. Weaver in the introduction to this issue. *See generally* Russell L. Weaver, *Privacy Discussion Forum: Introduction*, 17 FIU L. REV. 263 (2023).

autonomy of others. Yet the importance of protecting that core of people's lives means we must find a legal/technical curtain to protect those lives from the utter destruction of their privacy and right to personal autonomy.

I. INTRODUCTION: WHO ARE YOU?

Though Brandeis and Warren are often cited from their seminal 1890 law review article as positing that privacy was "the right to be let alone," they further set forth that privacy "was, as a part of the more general right to the *immunity of the person,—the right to one's personality*."[3] This notion of personal autonomy, inherent in Immanuel Kant's moral imperative of *Observantia*, the equal respect owed to all humans, is manifest in European regulation such as the General Data Privacy Regulation of the European Union. It is a possible regulatory framework for the United States, but the road to implementation is complex. This assumes treating all people as ends, not means, and in the messy democratic mudwrestling of competing interests in the U.S., such programs must fight their way to enactment and enforcement. The Federal Trade Commission (U.S.) is examining how its rulemaking powers may enable protective regulation in a variety of areas as to the prevalence of commercial surveillance and data security practices that harm consumers.[4]

In particular, the FTC is examining issues as to the need for new regulation as to how commercial entities:

> (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as
> (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.[5]

[3] Warren & Brandeis, *supra* note 1 (emphasis added).

[4] *Commercial Surveillance and Data Security Rulemaking*, FED. TRADE COMM'N (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

[5] *Id.*

Key here is how such efforts at new regulation of data collection and analytics will be received by the legislature and the judiciary. The United States Supreme Court has begun to rein in the regulatory power of federal agencies absent clear direction by the U.S. Congress of their powers and spheres of action. This is a key battleground between commerce, government, and the people. There is power and money in data, and both are powerful motivators for activity across multiple realms from commerce to politics. Data can be analyzed and composed to present a profile of a person for many different purposes that may enhance public safety, improve sales, and garner votes. There is so much to be learned from such surveillance via data analytics, from law enforcement to academic efforts to understand the tenor of America. Thus, publicly available online fora that have become standard loci for types of hate speech may be followed for analytical public safety.

An example of the power and scope and *profitability* of such data analytics is the U.S. web analytics firm Babel Street. Babel Street does massive examination of web data sources for its customers, taking *publicly* available data, such as from Instagram, to build such profiles.[6] Its clients include local, state, and federal law enforcement. Such profiles can support public safety in many ways. They may also create a surveillance state for the punishment of disagreement with authority.

The depth of revelation is seen in the adage "you are what you eat."[7] With major grocery businesses offering discounts in exchange for identification tagging of a person's purchases, they build data profiles of what a person may need and may want. These are key aspects of a personality that, in the past, were much more difficult to discern. For data empires such as the People's Republic of China, it can be used in innumerable ways for and against that data subject.

The risks are evident in the wake of the United States Supreme Court ruling in *Dobbs v Jackson Women's Health Organization*[8] that overturned precedents providing a limited constitutionally-protected right of a woman to terminate a pregnancy, an aspect of the personal autonomy of a woman as to her physical condition. This returned regulation of abortion—highly intrusive—to the several states, a number of which immediately enacted or activated laws with extensive restriction on such terminations. Other possible restrictions suggested were laws prohibiting citizens from traveling to other

[6] Aaron Gregg, *For This Company, Online Surveillance Leads to Profit in Washington's Suburbs*, WASH. POST (Sept. 10, 2017), https://www.washingtonpost.com/business/economy/for-this-company-online-surveillance-leads-to-profit-in-washingtons-suburbs/2017/09/08/6067c924-9409-11e7-89fa-bb822a46da5b_story.html.

[7] *See generally* JEAN ANTHELME BRILLAT-SAVARIN, PHYSIOLOGIE DU GOÛT (1825).

[8] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242 (2022).

states for such procedures; proposed legislation to permit such travel and shield those women has been blocked in Congress.[9] Soon after, data surveillance and analytics raised its head. Location data analytics firms began receiving requests for the identities of those who visited abortion clinics near state borders.[10] Tracking was done via *voluntarily shared* data from cell phones.[11] Related analytics against a database of purchases for targeted advertising let a woman's family to learn of her pregnancy before she told them.[12] The possibilities for broad surveillance across all of a person's activities seem endless.

This new expansion of possible uses of these vast data collections and associated AI analytical systems pushes the boundaries of personal privacy, personal autonomy, and personal security to the edge. These may lead to and *permit* invasions of privacy and other injuries that may flow from those invasions, even if, as concerned Warren and Brandeis, they are not cognizable as a violation of personal rights as to offer protection through the system of justice. These twins of big data and muscular analytics risk a dire impact on the social and political life of any person, from scorn to shunning to imprisonment for fifteen years.[13] Perspectives of the benefits and risk from such systems range to the future of policing and for predicting those who should be labeled enemies.[14] The void in U.S. privacy law has been filled piecemeal by various legislation, often keyed to particular industries such as health care and finance. The default protections under American common law are seen in the U.S. Restatement of Torts, 2d on Privacy as an enunciation

[9] Caroline Kitchener & Devlin Barrett, *Antiabortion Lawmakers Want to Block Patients from Crossing State Lines*, WASH. POST (June 30, 2022, 8:30 AM), https://www.washingtonpost.com/politics/2022/06/29/abortion-state-lines/; Trish Turner & Allison Pecorin, *Republicans Block Bill to Shield People Who Travel Out of State for Abortions*, ABC NEWS (July 14, 2022, 5:28 PM), https://abcnews.go.com/Politics/republicans-block-bill-shield-people-travel-state-abortions/story?id=86821057.

[10] Patience Haggin, *Phones Know Who Went to an Abortion Clinic. Whom Will They Tell?*, WALL ST. J. (Aug. 7, 2022, 8:03 AM), https://www.wsj.com/articles/phones-know-who-went-to-an-abortion-clinic-whom-will-they-tell-11659873781.

[11] *Id.*

[12] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=1f801c8a6668. Others dispute this, challenging the assertion that algorithms are that effective and played a role in this case. *See* Colin Fraser, *Target Didn't Figure Out a Teenager Was Pregnant Before Her Father Did, and That One Article That Said They Did Was Silly and Bad.*, MEDIUM (Jan. 3, 2020), https://medium.com/@colin.fraser/target-didnt-figure-out-a-teen-girl-was-pregnant-before-her-father-did-a6be13b973a5.

[13] Matt Mathers, *Russian Duma Passes Law Giving 15-Year Prison Sentences for Spreading "False Information" About Military*, INDEP. (Mar. 4, 2022, 9:37 AM), https://www.independent.co.uk/news/world/europe/ukraine-war-latest-russia-law-b2028440.html.

[14] Robert Davidson, *Automated Threat Detection and the Future of Policing*, FBI L. ENF'T BULL. (Aug. 8, 2019), https://leb.fbi.gov/articles/featured-articles/automated-threat-detection-and-the-future-of-policing; Ashley S. Deeks, *Predicting Enemies*, 104 VA. L. REV. 1529, 1530 (2018).

of American common law in this area. This secondary source of authority, mirrored by state caselaw enactment, sets out three areas of invasion relevant to data use under American common law: the intrusion upon seclusion, disclosure of private facts, and showing someone in a false light.[15] Analytics run against large data sets can injure people in each of these areas through the revelation of things best kept within a personal domain.

Government transparency in its data can exacerbate similar invasions of personal autonomy and the right to be left alone. Efforts by victims of domestic violence to escape their abusers and achieve the protection of seclusion and securing of private locational information have been thwarted by "government transparency." State motor vehicle agencies sold victims' driver's license locational information to their abusers, sometimes with fatal consequences.[16] With current address information mandated by state laws, this was only remediated by federal legislation making it illegal to reveal some types of data.[17] But states continue to mine and sell driver's license information, including to private investigators, leading some, such as the Electronic Privacy Information Center, to argue prohibitions on such dissemination need to be updated and strengthened.[18]

Risks abound, but are we willing to face them? Are we willing to legislate protections before more people suffer? What tradeoffs might we accept, and who will make whole those injured by these systems?

II. The Challenge to Personal Autonomy and Privacy: Should Something Be Done?

False light, disclosure of private facts and intrusion in the secluded protected places so valued by the Fourth Amendment can all be engendered through the data and analytics available. The State of Michigan's data system regarding unemployment compensation benefits produced flawed analyses labeling innocent people as fraudulently applying for benefits, leading to unwarranted legal action seizing their bank accounts and tax refunds.[19] As noted above, data analytics against a retailer's database of customer purchases, and the subsequent commercial solicitations generated thereby,

[15] Millar v. Taylor, [1769] 4 Burr. 2303, 2312 (Eng.).

[16] *Death of Actress Aided by State's Failure to Protect Data in 1989*, CAL. DEP'T OF CORR. & REHAB. (Sept. 3, 2020), https://www.cdcr.ca.gov/insidecdcr/2020/09/03/death-of-actress-aided-by-states-failure-to-protect-data/.

[17] The Drivers Privacy Protection Act, 18 U.S.C. § 2721 (1994).

[18] Joseph Cox, *DMVs Are Selling Your Data to Private Investigators*, VICE (Sept. 6, 2019, 9:09 AM), https://www.vice.com/en/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars.

[19] Cahoo v. SAS Analytics, Inc., 912 F.3d 887, 893–94 (6th Cir. 2019).

led by young woman's family to learn of her pregnancy before she told them.[20] And criminal prosecutions may await those who travel to other states to receive pregnancy termination services. Similar analytics against large data sets can, in effect, reveal what goes on behind closed doors regardless of any physical intrusion. It is akin to passive infrared scanning of the home barred under the Fourth Amendment (U.S.) as to protect people in *Kyllo v. United States*.[21] Flawed analytics can lead to the identification of the wrong person as a criminal suspect via facial recognition systems.[22] The sheer power of these systems may lead to misuse for wrongful purposes, even as systems for social control.[23]

The machine learning environment for self-taught pattern recognition has its own dangers where the existing data analyzed is flawed. Examples include the perpetuation of racial discrimination via analysis of past discriminatory outcomes that the machine strives to normalize to produce similar outcomes, not knowing of the wrongful intent of the past.[24]

Keller outlines the importance of addressing the collision between people's privacy versus transparency of information, whether with governmental or private entities.[25] She posits questions that should be addressed of what data needs be shared, especially as to personal information. She notes this, "pits privacy goals data-access and research goals" where privacy includes personal autonomy and control of data-access as essential.[26] But this may conflict with ever more effective and efficient operations of government, commerce, and the academy through access to such personal information.

The power of analytical systems, both to crunch the data and find patterns within it, may render ineffective any efforts to anonymize data as to make personal identification difficult. Techniques for the "anonymization" data can be circumvented by increasingly sophisticated algorithms and data matching systems, thus negating that which, on its face, seems to protect privacy while permitting broad data analysis.

[20] Hill, *supra* note 12; Fraser, *supra* note 12.

[21] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[22] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/.

[23] Sarah Valentine, *Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control*, 46 FORDHAM URB. L.J. 364, 392, 403, 406 (2019).

[24] James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 FORDHAM URB. L.J. 219, 232–34, 236–37 (2019).

[25] Daphne Keller, *User Privacy vs. Platform Transparency: The Conflicts Are Real and We Need to Talk About Them*, STAN. L.: CTR. FOR INTERNET & SOC'Y BLOG (Apr. 6, 2022, 6:00 AM), https://cyberlaw.stanford.edu/blog/2022/04/user-privacy-vs-platform-transparency-conflicts-are-real-and-we-need-talk-about-them-0.

[26] *Id.*

Consider the central role now played by the federal identifier of a person's Social Security Number, required for almost every civil action in U.S. society. The use of alphanumeric strings for databases encouraged its use across multiple platforms. Its compromise and misuse for identify theft can cause broad misery, from fraudulent commercial transactions to wrongful criminal prosecutions. The Social Security Administration itself notes the how that Social Security Number can be used to collect other personal data and be employed for identity theft.[27] One example of how this key datum may be compromised via analytics is the straightforward algorithm that takes a person's birth year and birth state to infer with high accuracy the first five numbers of the persons' Social Security ID; a significant number of full seven digit SSNs can be further inferred.[28] Another is Sweeny's finding that eighty-seven percent of U.S. residents can be identified if you have their birthdate, gender, and zip code.[29]

Keller fears that in the absence of an effective technical solution, legislative responses may do unnecessary damage in poorly considered "tiers of data access" trying to parse between academic, law enforcement, government and commercial interests. Statutory limitations on data elements might render some important work useless across multiple domains.

III. TRANSPARENCY OF GOVERNMENT: CHALLENGES AND DANGERS

Related to this is the need for transparency in the operations of AI systems and automated-decision-making, what some consider to be "explainable AI." Such transparent detail of analytics operations can be validated as to its reliability and error rates as to inferences. They can help assure accountability for injuries that can act to encourage good design and deep reduction in the errors such systems may generate. Those errors may lead to serious injuries, such as those detailed for the Michigan MiDAS system.

Felzmann et al., suggest as a solution that "Transparency by Design" can help assure effectiveness in systems and the transparency necessary to

[27] *Identify Theft and Your Social Security Number*, SOC. SEC. ADMIN. (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[28] Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L ACAD. SCI. 10975, 10975 (2009).

[29] *See* Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000).

judge their reliability.[30] Transparency promotes safety by making evaluation of systems easier.

They proposed a system to assure effective operations:

> 1) Proactive efforts to promote transparency;
> 2) Transparency must be integrated into the design of the system;
> 3) Clearly communicate and document operations within the system as to be clear to all stakeholders;
> 4) Detail what and how data is processed and the associated risks with this process;
> 5) Address issues of technical limitations on "explainability" of the operations of complex systems;
> 7) Assure the system can be inspected and audited as to its operations and outputs;
> 8) Respond to Stakeholder Issues, even if you don't like them;
> 9) Report on operations and issues with such operations.[31]

But technology companies may be hesitant to allow anyone to see how their products function as to lose their technological advantage via trade secret protection of intellectual property. One example of such concerns relates to blood alcohol breath testing equipment that has convicted so many people.[32] To integrate it into system design and document processes and operations are, at best, extra steps in understanding and documenting system development that slow down the process and irritate some programmers. Similarly, explaining the processes and analyzing risks with false positives and false negatives takes extra time, although essential to "explainability" of such systems; remediating technical limitations on this takes extra effort to fully understand the system beyond an immediate output as desired by the customers and sales staff. Others have suggested mandatory public audits of policing algorithms to minimize injuries to the innocent.[33] These proposals reflect support for the open source software movement that making the code open for public evaluation and analysis promotes better code and better, safe

[30] Heike Felzmann, Eduard Fosch-Villaronga, Christopher Lutz & Aurelia Tamò-Larrieux, *Towards Transparency by Design for Artificial Intelligence*, 26 SCI. & ENG'G ETHICS 3333, 3344 (2020).

[31] *Id.* at 3346–53.

[32] Stacey Cowley & Jessica Silver-Greenberg, *These Machines Can Put You in Jail. Don't Trust Them.*, N.Y. TIMES (Nov. 3, 2019), https://www.nytimes.com/2019/11/03/business/drunk-driving-breathalyzer.html; Aurora J. Wilson, *Discovery of Breathalyzer Source Code in DUI Prosecutions*, 7 WASH. J. L. TECH. & ARTS 121, 124–125, 132–133 (2011).

[33] Letter from Professor Tarik Aougab et al., to American Mathematical Society Notices, https://docs.google.com/forms/d/e/1FAIpQLSfdmQGrgdCBCexTrpne7KXUzpbiI9LeEtd0Am-qRFimpwuv1A/viewform.

computer programs; though some suggest validation of this is needed, it is acknowledged that simply opening the code and algorithms to inspection is an important step in information assurance and reliability.[34] Such validation of reliability is particularly important for AI systems and their outputs due, in part, to the expansion of massive data collections and cloud computing services.[35]

These extra efforts require time and money on the part of developers, middlemen, and users. They understandably may not wish to pursue these extra items that may cost but do not have an immediate return on investment, or possibly negative results where scrutiny reveals flaws in the system, such as with Michigan's MiDAS system for detecting unemployment insurance fraud. The development of tort liability relating to injuries from the systems to one's privacy can serve to create some incentive to prevent needless injury. Given the pace of the development of common-law and the novelty of the kinds of injuries that these systems can cause, legislative solutions may best address this globally.

IV. THE CHALLENGE OF ASSURING RELIABILITY AND PRIVACY FOR THE UNITED STATES

Matching technical and legal needs is the challenge. Yet, it is necessary to preserve the benefits of this technology for promoting public safety, justice, and equity.[36] The challenge may need both technical solutions.

Kapelke suggests differential privacy techniques can preserve privacy in the analysis of data, a technique whose use is growing.[37] The application of differential privacy methods adds to the base data some types of random information, akin to a salt in cryptographic keys, to obfuscate and confuse efforts at data matching to identify the data subject. Dwork et al., opined that such systems, though very effective, would benefit from transparency via an open source "Epsilon Registry" detailing how they are implemented as to

[34] Bev Littlewood & Lorenzo Strigini, *Software Reliability and Dependability: A Roadmap*, ICSE '00: PROC. ASS'N FOR COMPUTING MACH. (ACM) CONF. ON FUTURE SOFTWARE ENG'G, 175, 182 (2000), https://dl.acm.org/doi/pdf/10.1145/336512.336551.

[35] Sahil Suneja, Yunhui Zheng, Yufan Zhuang, Jim A. Laredo & Alessandro Morari, *Towards Reliable AI for Source Code Understanding*, SOCC '21: PROC. ASS'N FOR COMPUTING MACH. (ACM) SYMP. ON CLOUD COMPUTING, 403, 403 (2021), https://dl.acm.org/doi/pdf/10.1145/3472883.3486995.

[36] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 3 U. BOLOGNA L. REV. 180, 185, 195–196 (2018).

[37] Chuck Kapelke, *Using Differential Privacy to Harness Big Data and Preserve Privacy*, BROOKINGS (Aug. 11, 2020), https://www.brookings.edu/techstream/using-differential-privacy-to-harness-big-data-and-preserve-privacy.

promote understanding and implementation of effective and secure systems.[38]

The European Union has been forceful in detailing legislative protections under its General Data Privacy Regulation (GDPR). The United States, not so much, using a piecemeal approach by government and industrial sectors, sometimes after someone is injured. But the pending American Data Privacy and Protection Act[39] may offer a coherent legislative framework of protection, though there are concerns as to effective implementation; modeling it after the EU GDPR and the U.K.'s privacy statutes would offer tried and tested implementations as to facilitate protections for Americans.[40]

Further issues with data collection, storage, transmission, and processing under U.S. law are that they are all protected activities under the free speech protections of the United States. The First Amendment may protect the right to sense, collect, process and store data from the myriad transactions now caught via a myriad of systems. U.S. federal regulation may be possible under some interstate commerce regulatory powers, but those are also subject to constitutional limitations. In *Sorrel v. IMS Health Inc*., the Supreme Court found Vermont's Prescription Confidentiality Law limitations on the disclosure, sale, and use of prescription data to pharmaceutical companies by pharmacists an unjustified limit on First Amendment protections relating to content and speaker.[41] The Court distinguished this case of private parties dealing in data from *Los Angeles Police Dep't v. United Reporting Publishing Corp.*,[42] which upheld the denial of a facial challenge to restrictions on access to police information as the grounds for such a challenge did not present per *New York v Ferber*,[43] and it did not limit access to information held by private parties.[44]

Further, limitations on data processing and the algorithms that actuate it may also need to pass strict scrutiny as to content based restrictions. Although the Supreme Court has not spoken to the issue of First Amendment protections for code itself, several lower courts have found code itself

[38] Cynthia Dwork, Nitin Kohli & Deirdre Mulligan, *Differential Privacy in Practice: Expose Your Epsilons!*, 9 J. PRIV. & CONFIDENTIALITY 1, 3 (2019).

[39] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[40] Eric Cole, *The American Data Privacy and Protection Act's Potential Flaws and Implications*, CPO MAG. (July 25, 2022), https://www.cpomagazine.com/data-privacy/the-american-data-privacy-protection-acts-potential-flaws-and-implications/.

[41] Sorrell v. IMS Health Inc., 564 U.S. 552, 566, 577–580 (2011).

[42] *Id.* at 553.

[43] New York v. Ferber, 458 U.S. 747, 767 (1982).

[44] L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32, 39–41 (1999).

protected expression and subject to limitation surviving strict scrutiny for compelling reasons to restrict.[45]

The First Amendment creates a major hurdle for GDPR-like limitations on data revelations in the United States. There is a significant split as to how such limitations may be applied. Limitations on government activity have generally been upheld, such as restrictions on disclosure of stored electronic communications by private parties to government entities.[46] Limitations on private activity, as discussed above, will be much more difficult absent a showing of compelling need.

Deconstructing the areas of concern raise these questions; even where interstate commerce powers may permit federal regulation as well as inherent state powers with state regulation, both must comply protections on free expression the First Amendment.

A related factor is that common law privacy protections via tort liability rely on matters that are kept private. Public revelation of private facts from publicly available sources may not automatically invoke those protections. The Supreme Court noted "if a newspaper lawfully obtains truthful information about a matter of public significance[,] then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[47] The immense amount of data generated by peoples' lives, both voluntary and unknowing, create opportunities for inferential analysis and revelation.

Devising limitations on data sensing and collection to promote protections may be one option. Such data collection covers many domains, from private commercial transactions at a store scanner to activity in public areas. Past Fourth Amendment jurisprudence has found there is no "reasonable expectation of privacy" in such data collections, making them ripe targets for analytics.

But the intrusive power of analytics creates a number of indeterminate areas for regulation. The ruling in *Carpenter v. United States* by the Supreme Court, upended the doctrine that there was no reasonable expectation of privacy in data given to or legally collected by third parties. The Court held that law enforcement access to historical Cell Site Location Information (CSLI) from private providers, the functional equivalent of a personal tracking device, could only be had upon presentation of a warrant based on probable cause of criminal activity.[48] The Court found that the new technology of cellular telephones, their wide use and the precision of

[45] *See* Bernstein v. U.S. Dep't of State, 974 F. Supp 1288, 1306–07 (N.D. Cal. 1997).

[46] *See, e.g.*, 18 U.S.C. § 2701.

[47] Smith v. Daily Mail Pub. Co., 443 U.S. 97, 103 (1979); Fla. Star v. B.J.F., 491 U.S. 524, 524 (1989).

[48] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

locational data collected went too far in infringing what users would deem to have a reasonable expectation of privacy. Matching the privacy analyses from *United States v. Jones* and *Riley v. California* against older third party doctrines vitiating any such expectations, the Supreme Court invoked the expectations of privacy at the enactment of the Fourth Amendment to bar such data collection and analysis absent a warrant issued upon a showing of probable cause.

While limiting actions by state actors, this data would still be available to private parties for whatever purposes they choose. As the case of Babel Street shows, there is a market for such information privately. It may remain an open question as to whether state actors can access information from other sources, such as via Babel Street's open sources or private, for-profit data brokers. But the greater concern is that the privacy violations prohibited to the state by the Fourth Amendment may not invoke any sanctions if done by private parties. Yet, such private violations may carry their own injuries for those profiled by this data collection. This is especially true if published to others, whether by First Amendment publishers or the private channels powerfully enabled by social media and Internet technologies.

This further creates questions as to the propriety of sensing activity regarding the myriad of other devices generating data on personal activity, such as RFID chips and other collections of information. The Supreme Court case of *Kyllo v. United States*,[49] as well as *Carpenter v. United States*[50] and *Riley v. California*,[51] demonstrated yet again that the Fourth Amendment privacy protections of the Constitution protect people, not places, even from passive data collection by infrared sensors. The massive data people generate on their lives that is collected and subject to analytics can be more informative than the images in *Kyllo* and the general locational data in *Carpenter*. It moves the monitoring of people closer and closer to real-time surveillance that, in the past, required significant resources to perform and decisions as to the wisdom of using such limited resources.

Limitations on storage and transmission, as *Sorrel* demonstrated, may not apply to private parties storing and transmitting information absent meeting a strict scrutiny test upon a showing of a compelling need. This may require the evolution of reasoning in support that there is a compelling need for the protection of people through such limitations.

Differential protections in law may be possible, as shown by constitutional prohibitions on limiting pornography to adults but permitting such limitations as to access by minors. This "compelling interest" in the

[49] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[50] *Carpenter*, 138 S. Ct. at 2221.

[51] Riley v. California, 573 U.S. 373, 381 (2014).

protection of children may be a starting point for regulation, but it is necessary that access by adults not be hindered. There are ways to accomplish both.

While limitations on data processing for governmental purposes may be possible, it is difficult to see such limitations applied to private parties absent passing the review of strict scrutiny. This is particularly true where we are examining the application and output of algorithms, the essential part of computing machinery that tells us what we want to know. Yet such limitations are part of EU limits via the GDPR[52] which impact U.S. entities processing data on EU citizens. These may help bootstrap such protections in some circumstances.

It seems under United States law, that limitations on private parties and their use of data and data processing can only be limited on a showing of a compelling need and narrowly drawn means effective to accomplish that compelling need. Other regulatory mechanisms may come into play, however. The First Amendment does not protect "non-speech," expression that falls; these may include:

> 1) Statements placing someone in a false light;
> 2) Disclosure of private facts not of public interest, perhaps, though declining;
> 3) Statements that are defamatory; and
> 4) Statements that are erroneous and injure someone in their rights.

Personal autonomy rights, such as sanctions for depicting someone in a "false light" or to defame them, may still be enforced. Related data processing that falsely indicates wrongdoing as to lead to wrongful punishment of an individual may also be sanctioned.[53] While these *post hoc* remedies do not anticipate injuries and means to remediate, the threat of such offer some deterrence to unreflective use of insufficiently vetted systems that hurt others.

These may also provide a foundation for regulation that survives First Amendment limitations on actions. Combined with other concerns, such as regulation of safe products and systems generally, perhaps this will permit an appropriate regime to assure privacy in this computational age.

The related regime of false light, and regulations relating to fairness and non-discrimination, must be part of any regulatory scheme. The Federal Trade Commission (FTC) has extensive regulatory engagement with

[52] Regulation 2016/679, of the European Parliament and of 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, 2016 O.J. (L 119) 1–88.

[53] Cahoo v. SAS Analytics, Inc., 912 F.3d 887 (6th Cir. 2019).

businesses over the security of their data, given the broad damage to consumers compromise might entail. It can have similar authority over data processing as to impacts on consumers as part of information assurance. Its workshop and subsequent report, "Big Data: A Tool for Inclusion or Exclusion," set out parameters for consideration as to maximization of benefits and minimization of the harms that may come from massive data sets reviewed by powerful analytics.[54] The FTC report suggests that companies using such data services address these issues:

1) How representative is your data set?
2) Does your data model account for biases?
3) How accurate are your predictions based on big data?
4) Does your reliance on big data raise ethical or fairness concerns?[55]

These accord with the concerns raised as to the utility and fairness of AI-driven facial recognition systems, that these systems still had a significant potential of injury through misidentification and false attribution.[56] IBM ended its commercial efforts with facial recognition systems due to concerns with discrimination and unjust use.[57] IBM Chief Executive Officer stated in a letter to Congress:

> IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency. We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies.[58]

Shilling acknowledges diminishment of privacy rights from both First Amendment doctrine and the factual changes wrought by the new information technologies of the Internet and social media.[59] Yet she posits

[54] *See generally* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[55] *Id.* at iv–v, 27–32.

[56] AXON ENTER., INC., FIRST REPORT OF THE AXON AI & POLICING TECHNOLOGY ETHICS BOARD, 32, 37–38 (2019), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d13d7e1990c4f00014c0aeb/1561581540954/Axon_Ethics_Board_First_Report.pdf.

[57] Aimee Chanthadavong, *IBM Announces Exit of Facial Recognition Business*, ZDNET (June 8, 2020), https://www.zdnet.com/article/ibm-announces-exit-of-facial-recognition-business/.

[58] Arvind Krishna, *IBM CEO's Letter to Congress on Racial Justice Reform*, IBM (Nov. 11, 2020), https://www.ibm.com/policy/facial-recognition-sunset-racial-justice-reforms/.

[59] Kirby Shilling, *Bad Publicity: The Diminished Right of Privacy in the Age of Social Media*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 756, 756 (2022).

that protection from public disclosure of private facts is not dead, but in need of the clarity of statutory protections both for the data subject and the data publisher. Statutory liability might be built upon limits on data access, such as the illegal interception of electronic communications, and definition of compelling state interests—"of the highest order"[60]—such as child protection and limitations on prurience, as to give notice of protected areas for both data subject and data publisher.

It is time to begin a national dialogue on the scope and power of massive data and powerful analytics and the impact on our peoples. The impact on the lives of us and of others may be destructive of that which holds us together.[61]

V. CONCLUSION

Our new computational regime of data and analytics in this Internet Age have opened unprecedented windows into the lives, thoughts and even souls of people. As Justice Sotomayor opined, such surveillance powers may change the relationship between citizens and the government, and then extended to relationships between people and their society.[62]

Although open windows may destroy a reasonable expectation of privacy in one's home, curtains may be used to regain it. In the transparency that data provides under algorithmic processing, we must come up with curtains to protect the lives of people as appropriate and permissible. That may best be engendered by statutory protections from legislative bodies, including appropriate guidance to regulatory agencies for effective rulemaking.

Limitations on data collection may begin that process, although it, too, must address First Amendment protections over the right to receive and collect information. Limitations on how that data is processed and the revelations and use thereof that come from it must similarly address those concerns. Limitations on data collection and processing on children demonstrate a starting point for jurisprudence. Other areas of data regulation will follow. This can create a foundation for people to learn to protect themselves in adulthood and to know that they should not leave everything about their lives lying around. An interesting future is ahead of us. It may very well require we reevaluate what we mean by privacy, self-protection, and personal autonomy.

[60] Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989).

[61] United States v. Jones, 565 U.S. 400, 413–18 (2012) (Sotomayor, J., concurring).

[62] *Id.* at 416.