Confidentiality Creep and Opportunistic Privacy

David S. Levine*

> However new and astonishing one's surroundings, the tendency is to become a part of them so soon that almost from the first the power to see them objectively and fully measure their strangeness is lost.[1]

 Associate Professor, Elon University School of Law; Affiliate Scholar, Stanford Law School Center for Internet and Society. This Article significantly expands upon my introduction of "confidentiality creep" in a Freedom to Tinker blogpost from August 2015. *See* David Levine, *The Chilling Effects of Confidentiality Creep*, FREEDOM TO TINKER (Aug. 1, 2015), http://freedom-to-tinker.com/2015/08/01/the-chilling-effects-of-confidentiality-creep/. Additionally, this Article is inspired by the work of Frank Pasquale, as well as many conversations and ideas that we have discussed over the past several years. Indeed, the phrase "opportunistic privacy" derives from Pasquale's identification of amorphous application issues in privacy, similar to those about which I have written in trade secrecy. Particularly in Part I and Section II.A, *infra*, some ideas and textual structure derive from Pasquale's contributions to our prior unpublished project regarding trade secrecy and access to information. Where those ideas and structure come from that project, they are footnoted. I thank Pasquale for his permission to run with these ideas, as well as his many suggestions and insights. Additionally, I am grateful for the extensive research performed by Merima Mustafic, particularly reflected in this Article's discussion of algorithmic computing, as well as research and citation support by Rebecca Kilmon, Caitlin Mitchell, Kalie Pritchett, and Rachel Stariha. For comments throughout the research and writing process, thanks to Bruce Boyden, Ed Felten, Elizabeth Townsend Gard, Todd Gers, Irina Manta, Tim McFarlin, Kali Murray, Arvind Narayanan, and participants at Yale Law School's Unlocking the Black Box conference, the 2017 Association of American Law Schools Annual Meeting Computer and Internet Law Section panel, Hofstra Fall 2017 Intellectual Property Colloquium, and the 2016 Intellectual Property Scholars Conference. Finally, thanks to this *Journal*'s editors and staff for their excellent work. This Article is supported, in part, by a grant from Elon University's Turnage Fund. Of course, all errors and omissions are my own. This Article is current as of November 1, 2017.

1. EDWARD BELLAMY, LOOKING BACKWARD 120 (Penguin ed. 1986) (1888).

I. INTRODUCTION

In Edward Bellamy's 19th century vision of a utopian United States in the year 2000, man has attained perfection through, in part, his access to knowledge. Bellamy's protagonist, Julian West, awakens from over 100 years of sleep to find himself in the year 2000, comparing his "former life" to the "strangeness of [his] present environment."[2] As part of his welcome and reorientation to his new world, he is led to a library filled with his "friends," the books by the "great writers of my time and all time."[3] As he was writing in the 1880s, Bellamy undoubtedly understood the power that knowledge affords and sought its wider access as an utopian way to address the social and economic challenges of the last quarter of the 19th century.

While Bellamy's vision of knowledge utopianism has not yet been realized (despite the idealism of the Internet's early visionaries),[4] the power of technology to pull its users uncritically into its morass has never been more profound. We are mesmerized by an endless stream of immersive content on Facebook and by the car that moves but lacks a human driver. Yet, as a society, we rarely pause to understand their strangeness, as these technologies seem beyond our collective grasp, or even willingness, to comprehend. They work, they make our lives better, and others know how to build them. That's good enough, we surmise; but should the public need to know more about how they work and their capabilities?

This Article's implicit answer is "yes," and it highlights an emerging impediment to the ability to fully see and objectively measure today's new technologies. Increasing amounts of secret and proprietary information, known by few, impede the public's interest in an open democratic society where, as Bellamy foresaw, understanding strangeness is paramount. More specifically, within the past five years, there has been a growing recognition that confidentiality and privacy designations on information can have a significant impact on the public's ability to know what private industry, and increasingly the government, is doing.[5] From the chemical formulas in hydraulic fracturing to algorithms

---

2. *Id.*

3. *Id.* at 119.

4. *See, e.g.*, John Perry Barlow, *The Economy of Ideas*, WIRED 1, 9 (Mar. 1, 1994, 12:00 PM), http://www.wired.com/1994/03/economy-ideas/ (emphasizing the nascent idea that "[i]nformation [w]ants to [b]e [f]ree," and specifically recognizing the "natural desire of secrets to be told and the fact that they might be capable of possessing something like a 'desire' in the first place"). See Part II for discussion of issues raised in this paragraph.

5. *See, e.g.*, Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1151 (2008)

in autonomous cars, search engines, and social media, the demands of confidentiality and privacy have prevented the public from receiving critical information held by the private sector.[6] This putative confidential and private information is needed in order to understand how private behavior impacts the public.

This Article identifies two recent information control developments and the challenges that they present. The first is "confidentiality creep"—the quiet, under-scrutinized, amorphous expansion of the kinds of information deemed inappropriate for public consumption; the second is "opportunistic privacy"—the dubious use of privacy law and principles as an information control tool. Through examples deriving from the deployment of driverless cars and social media information diffusion, the problem can be seen more clearly.

This issue raises a classic problem that has been the focus of prior articles; namely, how to balance the public interest in information access and understanding, with the myriad reasons—from privacy interests to the utilitarian theory underlying intellectual property law—for understandably withholding information from the public.[7] As algorithms and code-based systems make private decisions that cause public harms,[8] accurate and thorough information is required for public understanding and governance. For example, few can see the process that allows an autonomous car to apply its brakes. However, that decision is in fact made somewhere and somehow, and there must be a reasonable way for that decision to be understood outside of the small circle of individuals

---

(examining "search engines' power to manipulate their results, thereby affecting the ability of Internet communicators to reach potential audiences"); Kathleen Feuer, Protecting Government Secrets: A Comparison of the Espionage Act and the Official Secrets Act, 38 B.C. INT'L & COMP. L. REV. 91, 93 (2015) ("The inappropriateness of the response to government employees who leak confidential information, whether regarded as traitors or whistleblowers, and the efficacy of the government's renewed efforts to stamp them out has reignited a national debate between two seemingly irreconcilable values: the government's need for secrecy and the people's right to know."); David S. Levine, *The People's Trade Secrets?*, 18 MICH. TELECOMM. TECH. L. REV. 61, 64 (2011) (arguing that the government should not have the power to say that information about public expenditures is a trade secret, and thus, should not be able to keep such information from the public).

6. *See infra* Part II.

7. *See* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 135 (2007) (arguing that, despite good reasons for maintaining trade secrecy in private commerce, "basic democratic values of transparency and accountability should prevail[]" when applied to the provision of public infrastructure); Levine, *supra* note 5, at 67 (arguing that state governments should be more transparent and accountable to the public, especially as it pertains to "information created entirely by the government and designated as trade secrets by the government itself").

8. Examples of public harms include online privacy invasions, as well as the physically manifesting harms resulting from such invasions.

and private entities that are directly responsible for, and benefit from, the decision.

Information controlled by those with vested interests in its secrecy creates classic moral hazard problems that are exacerbated by the complexity of the technologies now being deployed. Identifying the indirect and nascent costs from information bottlenecks is a daunting task. Indeed, even under ideal conditions, the law has a hard time keeping up with technological changes driven by pecuniary gain, much less engrafting optimal public understanding, into the equation.[9] We usually only identify the need for information after a harm has manifested.

Thus, when Uber was able to near-unilaterally decide when to begin testing autonomous cars in Pittsburgh, everyone played catch up, while Uber began its technological integration.[10] Similarly, Facebook had significant latitude regarding what to tell Congress and the public about alleged Russian manipulation of Facebook advertising in order to favor a presidential candidate, as well as the conditions for such sharing.[11] As a general matter, we are left with little choice but to hope that Facebook and Uber are sufficiently concerned about their public perception and market position so as to share useful information about the safety risks

---

9. *See, e.g.*, Kevin E. Davis, *Contracts as Technology*, 88 N.Y.U. L. REV. 83, 112 (2013) (discussing innovation within contract law, arguing that "it is important to distinguish between third parties who are motivated to innovate by the prospect of direct pecuniary gains, and third parties . . . that are motivated by other factors"); Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), http://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/ (arguing that "regulatory gaps exist because laws have not kept up with advances in technology").

10. *See infra* Part II.

11. *See infra* Part II. Facebook eventually provided a sample of the advertisements allegedly purchased by Russian entities to Congress, which released them to the public. As explained by *The Washington Post*,

> The ads that emerged, a sampling of the 3,000 that Russians bought during the 2016 presidential campaign and its aftermath, demonstrated in words and images a striking ability to mimic American political discourse at its most fractious. The targeting information also showed a shrewd understanding of how best to use Facebook to find and influence voters most likely to respond to the pitches.

Craig Timberg et al., *Russian Ads, Now Publicly Released, Show Sophistication of Influence Campaign*, WASH. POST (Nov. 1, 2017, 7:51 PM), http://www.washingtonpost.com/business/technology/russian-ads-now-publicly-released-show-sophistication-of-influence-campaign/2017/11/01/d26aead2-bf1b-11e7-8444-a0d4f04b89eb_story.html?tid=ss_mail&utm_term=.1ed5a94730ca. "Ordinary free posts by Russian-backed Facebook groups," which is the bulk of the influence efforts, were not shared or released. *Id.*

associated with autonomous automobiles on public roads and the very outcome of our presidential election process.[12]

Being beholden to vested information interests, backed by generalized law that does not draw distinctions based upon public interest in information, is needlessly problematic. Should Uber primarily determine when and how such deployment should occur, and who should bear the risks of that deployment, or should lawyers and technologists be able to weigh in on its timeliness throughout a regulatory process? Should Facebook decide what information the public needs in order to assess the veracity of a given story and whether to consider such information prior to casting a vote?

Moreover, as Facebook is already in the marketplace, and Google and Uber are already testing their autonomous cars on public roads, technological integration into society is underway.[13] But the moment that Uber or Facebook takes the lead in controlling the information most needed to assess the merit of their own decisions with external consequences and costs, everyone else takes the proverbial back seat. Thus, confidentiality creep and opportunistic privacy can provide or maintain the information dominance necessary for questions or concerns to remain "unanswerable," even as the technology becomes increasingly adopted.

These issues suggest the core problem identified in this Article—confidentiality creep and opportunistic privacy can allow emerging technologies to move beyond the sphere of observation, control, and law, creating an empty space in which the information most needed to understand technological activity is held only by those with a vested interest in the technology's rapid dominance. As a result, the groups that might temper unwarranted enthusiasm in the public interest—regulators, civil society activists, lawyers, academics, and technologists—run the risk of marginalization.[14] Information becomes captured and controlled at all levels of interaction: creative, political, regulatory, and social.

---

12. *See infra* Part II. To some degree, public pressure has compelled more transparency from Facebook already. Under increasing public scrutiny, Facebook recently announced new advertising policy guidelines, designed to help "protect the integrity of the electoral process." Rob Goldman, *Update on Our Advertising Transparency and Authenticity Efforts*, FACEBOOK NEWSROOM (Oct. 27, 2017), http://newsroom.fb.com/news/2017/10/update-on-our-advertising-transparency-and-authenticity-efforts/. Still, as discussed more thoroughly in Part II, dubious confidentiality and privacy claims and concerns remain.

13. *See infra* Part II.

14. This subject is the focus of my current early project entitled *Public Data Science*. Ed Felten generally refers to this issue as an "explainability problem." Ed Felten, *What Does It Mean To Ask for an "Explainable" Algorithm?*, FREEDOM TO TINKER (May 31, 2017), http://freedom-to-tinker.com/2017/05/31/what-does-it-mean-to-ask-for-an-explainable-algorithm/

While we might hope that such concerns would act to counter confidentiality creep and opportunistic privacy, fear of leakers like Julian Assange,[15] Chelsea Manning,[16] and Edward Snowden,[17] along with those behind the Ashley Madison,[18] Democratic National Committee,[19] Equifax,[20] and Sony Entertainment[21] hacks, suggest that the claims to and power of confidentiality and privacy as an argument will only grow, even as the power to maintain that confidentiality and privacy erodes. Indeed, the 2016 congressional report regarding Edward Snowden did not identify any regulatory interests in adjusting to the reality of leakers or viewing them as beneficial to public knowledge and debate; rather, Snowden was defined solely as a unitary threat to centralized control

("The first type of explainability problem is a *claim of confidentiality*. Somebody knows relevant information about how a decision was made, but they choose to withhold it because they claim it is a trade secret, or that disclosing it would undermine security somehow, or that they simply prefer not to reveal it. This is not a problem with the algorithm, it's an institutional/legal problem.").

15. *See* Mark Fenster, *Disclosure's Effects: WikiLeaks and Transparency*, 97 IOWA L. REV. 753, 758-59 (2012) (detailing WikiLeaks's unauthorized, mass disclosure of classified documents stolen from the U.S. government, released by Julian Assange, the most prominent figure behind WikiLeaks).

16. *See* Lauren Effron & Nadine Shubailat, *Chelsea Manning Explains Why She Leaked Secret Military Documents, Fought for Transgender Rights Behind Bars*, ABC NEWS (June 9, 2017, 7:39 AM), http://abcnews.go.com/US/chelsea-manning-explains-leaked-secret-military-documents-fought/story?id=47931325 (describing Chelsea Manning, formerly known as Bradley Manning, and the reasoning behind her unauthorized dissemination of confidential and sensitive U.S. military documents).

17. *See* Margaret B. Kwoka, *Leaking and Legitimacy*, 48 U.C. DAVIS L. REV. 1387, 1397-1400 (2015) (detailing Edward Snowden's 2013 leak of sensitive national security information, especially information regarding the extent of National Security Agency surveillance activities, both domestic and abroad).

18. *See* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (reporting on the hack, and subsequent information leak, committed by "[h]ackers who stole sensitive customer information from the cheating site," Ashley Madison, effectively outing 32 million married individuals who were on the site seeking partners for affairs).

19. *See* Patrick Lawrence, *A New Report Raises Big Questions About Last Year's DNC Hack*, NATION (Aug. 9, 2017), http://www.thenation.com/article/a-new-report-raises-big-questions-about-last-years-dnc-hack/ (asserting that the "remote hacks" of the Democratic National Committee's (DNC) mail system, which was attributed to Russians acting on behalf of Donald Trump during the 2016 presidential election, may actually have been a "leak" committed by an insider with access to sensitive DNC information).

20. *See* Erica R. Hendry, *How the Equifax Hack Happened, According to Its CEO*, PBS (Oct. 3, 2017, 9:43 AM), http://www.pbs.org/newshour/rundown/equifax-hack-happened-according-ceo/ (reporting on the Equifax data breach "that exposed the personal data of more than 143 million consumers").

21. *See* Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), http://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.84b895df5813 (detailing the hack into the computer systems of Sony Pictures Entertainment, in which "[t]he attackers stole huge swaths of confidential documents from the Hollywood studio and posted them online").

over information.[22] This trend is likely to continue into the foreseeable future.

Yet, identification of confidentiality creep and opportunistic privacy, as well as the recognition of leakers, are not licenses to render all information public. We have good reason to be skeptical of "radical transparency"—the idea that all information should be public.[23] Nonetheless, without understanding the nature of these information access threats—and more broadly, what information the public needs, wants, and doesn't need, and why—we risk losing public trust in facts themselves. How do we really know what is true if the core information needed to make such an assessment is inaccessible?

Thus, as confidentiality creep and opportunistic privacy continue to be utilized, confidence in the efficacy of public discourse will erode, and poorer policy decisions will result. Logically, if critical information can be hoarded and hidden by an interested few, for reasons that are not apparent to the outside world, why should the public even bother trying to make sense of that information, that "strangeness"? Since facts are obscured for dubious reasons, should we not just as well rely on the pundits and "spin doctors," who can opine on what we can see, like political maneuverings and press releases? Indeed, why discuss these questions at all? The remainder of this Article identifies examples of confidentiality creep and opportunistic privacy and suggests possible implications and reactions.

II. IDENTIFYING THE PROBLEM

Technological transparency does not naturally arise from wide adoption and use because information about a technology's operations may be wholly inaccessible even when the technology is utilized. Thus,

---

22. *See* HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, REVIEW OF THE UNAUTHORIZED DISCLOSURES OF FORMER NATIONAL SECURITY AGENCY CONTRACTOR EDWARD SNOWDEN, H.R. REP. NO. 114-891 (2016); David S. Levine, *Intellectual Property Without Secrets*, *in* 2 THE LAW OF THE FUTURE AND THE FAILURE OF LAW 337, 337 (Sam Muller, Stavos Zouridis, Morly Frishman & Laura Kistemaker eds., 2012) (discussing the implications of eroding the ability to maintain trade secrets).

23. By definition, radical transparency rejects all reasons—good or bad—for keeping information secret. *See generally* Luke Justin Heemsbergen, *Radical Transparency in Journalism: Digital Evolutions from Historical Precedents*, 6 GLOBAL MEDIA J. 45, 46 (2013) (exploring "how radical instances of transparency that are exploited and reported by journalists, become institutionalized in democracy," and providing a comparative analysis of the effects of recent instances of radical transparency); Steven A. Aftergood, *Wikileaks Fails "Due Diligence" Review*, FED'N AM. SCIENTISTS (June 28, 2010), http://fas.org/blogs/secrecy/2010/06/wikileaks_review/ (criticizing Wikileaks for engaging in "information vandalism," as it "routinely tramples on the privacy of non-governmental, non-corporate groups for no valid public policy reason").

encouraging access to information needed to improve public understanding often needs a regulatory nudge. To access usable and accurate information, there are a few primary options. First, those who are interested can rely upon outside experts to try to deconstruct or reverse engineer the technology at issue. Those individuals, however, may have their own legal and structural problems in engaging in that work.[24] Andrea Matwyshyn's recent successful effort to convince the U.S. Copyright Office that computer security researchers should not have to run afoul of copyright law in order to conduct research was designed not to achieve copyright infringement but rather to "spark a new era of benevolent hacking for both research and repair."[25] However, as Wired points out, researchers can still run afoul of the Computer Fraud and Abuse Act,[26] as well as trade secret law, so the legal path to access is far from clear (to say nothing of the engineering hurdles).[27]

Alternatively, one could look to reporters through intermediaries like *Bloomberg Businessweek*, *Consumer Reports*, ProPublica, or Techdirt in order to ascertain what is transpiring in one's social media feed or car. Nevertheless, when it comes to secret decision-making mechanisms, it is not even possible to assess the assumptions and values built into the algorithms that animate such decisions. This is a problem within algorithmic computing that is now gaining acknowledgment,[28] and which plagues scientific inquiry, as Victoria Stodden has demonstrated.[29] If Facebook's algorithms use an image from a user's account displaying a posted comment that threatens rape of the user to drive up Instagram

---

24. *See, e.g.*, Ed Felten, *Trade Secrets and Free Speech*, FREEDOM TO TINKER (Aug. 26, 2003), http://freedom-to-tinker.com/2003/08/26/trade-secrets-and-free-speech/ (asserting that, for example, very few engineers can actually understand fully Space Shuttle wing structure, and similarly, very few accountants are able to interpret Enron's finances in its raw form). Ideas and structure in this and the following three paragraphs derive from the prior unpublished project identified in the biographical footnote *supra*.

25. Andy Greenberg, *It's Finally Legal To Hack Your Own Devices (Even Your Car)*, WIRED (Oct. 31, 2016, 9:20 PM), http://www.wired.com/2016/10/hacking-car-pacemaker-toaster-just-became-legal/.

26. Computer Fraud and Abuse Act § 2, 18 U.S.C. § 1030 (2012).

27. *See* Greenberg, *supra* note 25.

28. *See generally* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PENN. L. REV. 633, 689 (identifying ways in which further research can "help to address the problem of unfairness in big data analysis"). Full access to source code is also not a panacea for full understanding. *See id.* at 638 ("Perhaps the most obvious approach is to disclose a system's source code, but this is at best a partial solution to the problem of accountability for automated decisions.").

29. Victoria Stodden, Sch. Info. Scis., Univ. Ill. Urbana—Champaign, Presentation at Social and Decision Analytics Laboratory Seminar: The Importance of Scientific Reproducibility in Evidence-Based Rulemaking (Dec. 2, 2015), http://web.stanford.edu/~vcs/talks/SDAL-Dec2-2015-STODDEN.pdf.

subscriptions,[30] what other bad decisions are being made with algorithms, and how would we know about those decisions anyway?[31]

Even if the above two options fail, one would expect regulators to at least have access to relevant information, and through that access, make intelligent regulatory decisions. Those decisions, based upon evidence and facts, would then be shared with the public and hopefully explained. However, as discussed below, our regulatory regime may leave blind spots, even intentionally. For example, Congress asked Facebook for access to relevant content in order to assess Russia's impact on our presidential election result and efforts to promulgate cyberwarfare, to say nothing of access to its algorithms (that might help us understand how and to whom such content is shown).[32] Due to a lack of expertise available to the government, especially with regard to new technologies, regulators may act based upon educated guessing, relying primarily on interested lobbyists for policy substance and legislative drafting.[33]

While the above examples outline the primary and imperfect avenues for public understanding, they still assume a rigorous system that allows for justifiable separation of the information that the public would need to know, would like to know, and cannot know. Alas, in many sectors, we lack such precision.[34] Thus, we are left with two fundamental questions; namely, (a) how can we attain access to the information needed to understand new technology at more than a general level, and (b) what reasonable impediments exist to that access? Confidentiality creep and opportunistic privacy are part of the answer.

---

30. Adam Clark Estes, *Facebook Used an 'I Will Rape You' Image To Invite Users to Instagram*, GIZMODO (Sept. 21, 2017, 6:29 PM), http://gizmodo.com/facebook-used-an-i-will-rape-you-image-to-invite-users-1818638390.

31. *See, e.g.*, U.S. Defense Secretary Donald Rumsfeld, Press Conference at the NATO Headquarters (June 6, 2002), http://www.nato.int/docu/speech/2002/s020606g.htm (detailing Defense Secretary Rumsfeld's famous "unknown unknowns" speech) [hereinafter Rumsfeld Press Conference].

32. *See infra* Section II.C.

33. *See, e.g.*, Ailsa Chang, *When Lobbyists Literally Write the Bill*, NPR (Nov. 11, 2003, 2:03 PM), http://www.npr.org/sections/itsallpolitics/2013/11/11/243973620/when-lobbyists-literally-write-the-bill (discussing the extent to which lobbyists influence legislation, and arguing, specifically, that lobbyists "often write the actual bills—even word for word"). *See generally* David Levine, *Bring in the Nerds: Secrecy National Security and the Creation of International Intellectual Property Law*, 30 CARDOZO ARTS & ENT. L.J. 105 (2012).

34. *See, e.g.*, Lee Rainie & Janna Anderson, *Theme 7: The Need Grows for Algorithmic Literacy, Transparency and Oversight*, PEW RES. CTR. (Feb. 8, 2017), http://www.pewinternet.org/2017/02/08/theme-7-the-need-grows-for-algorithmic-literacy-transparency-and-oversight/ (offering a variety of ideas about how everyday individuals "and the broader culture might respond" to the increasing use of algorithms, and discussing the need for greater public algorithm literacy, so as to hold the experts who create algorithms accountable to the general public).

A. The Context: Trade Secrecy

Part of the story of the attack on the public's right to know basic features of its technology ecosystem, and increasingly the government itself, is the growth of amorphous confidentiality and privacy claims. Within intellectual property law and information law, more broadly, this is a problem largely unique to the law of trade secrecy. Indeed, this Article posits that the root of identifying these issues derives from understanding how information access has been impeded by trade secret law.

Trade secret law operates very differently from its intellectual property cousins. For example, although abstract ideas are patentable, patent law limits the power of such protection.[35] Within copyright law, distinctions between the protection of ideas and facts, versus expressions and those considered fair uses, allow for the existence of a public domain made up of works of authorship that can be freely created and/or used by the public without limitation.[36] Of course, trademarks, by definition, must be accessible to be of primary use.[37]

Trade secrecy is a different beast entirely. From an information *access* perspective, as opposed to *use* perspective, trade secrecy is by far the most powerful intellectual property law. Trade secrets (including knowledge of their very existence) can last indefinitely and are difficult to limit, absent independent discovery (or some other form of disclosure) or reverse engineering.[38] Additionally, the most pervasive supposed limiting principle for trade secrecy is theoretical and often forgotten, namely, the utilitarian "incentives to innovate" rationale.[39] Indeed, the power to protect commercial secrets through trade secret law may

---

35. *See* Timothy R. Holbrook, *Method Patent Exceptionalism*, 102 IOWA L. REV. 1001, 1003 (2017) (discussing the unique limiting rules that apply to process or method patents versus product patents). Ideas in this paragraph derive from the prior unpublished project identified in the biographical footnote *supra*.

36. *See More Information on Fair Use*, COPYRIGHT.GOV (Sept. 2017), http://www.copyright.gov/fair-use/more-info.html.

37. Except in the case of keyword advertising. *See generally* Eric Goldman & Angel Reyes III, *Regulation of Lawyers' Use of Competitive Keyword Advertising*, 2016 U. ILL. L. REV. 103; Eric Goldman, *More Evidence Why Keyword Advertising Litigation Is Waning*, TECH. & MARKETING L. BLOG (Dec. 27, 2016), http://blog.ericgoldman.org/archives/2016/12/more-evidence-why-keyword-advertising-litigation-is-waning.htm; Eric Goldman, *Trademark Owners Just Can't Win Keyword Advertising Cases*—EarthCam v. OxBlue, TECH. & MARKETING L. BLOG (Sept. 28, 2014), http://blog.ericgoldman.org/archives/2014/09/trademark-owners-just-cant-win-keyword-advertising-cases-earthcam-v-oxblue.htm.

38. *See* JOHN R. THOMAS, CONG. RESEARCH SERV., R41391, THE ROLE OF TRADE SECRETS IN INNOVATION POLICY 6 (2014), http://fas.org/sgp/crs/secrecy/R41391.pdf.

39. *See id.* at 1 (discussing the importance of protecting trade secrecy to encourage innovation).

sometimes be an assumed necessity for innovation to occur when, in fact, it may not be necessary.[40]

If the utilitarian basis for trade secrecy is missing, the reasons to maintain trade secrets diminish significantly. Nonetheless, it is difficult to find any suggestion that trade secrecy should be limited as a result. Thus, reverse engineering[41] and independent discovery[42] are not effective as external trade secret limiting doctrines when the public has an interest in information access, given that such interest is absent from the trade secret calculus.

As discussed more fully below, both confidentiality creep and opportunistic privacy limit access to technological information in similar ways, and with similarly few meaningful checks on their power. Like trade secrecy, confidentiality and privacy are often assumed requirements for information access and use, and thus impede access to and use of the information at issue, even when the need for confidentiality or privacy in such information has not been fully established or examined.[43] Thus, at least at a top level, trade secrecy, confidentiality creep, and opportunistic privacy can lead to the same informational blind-spots.

At a deeper level, like trade secrecy, both confidentiality and privacy have amorphous theoretical underpinnings.[44] Akin to trade secrecy's frenetic reasons for existing, because of the similarly amorphous nature of the privacy concept, it is difficult to pin down where its limits may be set beyond Warren and Brandeis' famous conception of it as a "right to be let alone."[45] As for confidentiality, it is

---

40. *See id.* at 4 ("[A]lthough trade secret law may promote advancement, it might facilitate a particular kind of innovation—the development of information that is itself amenable to being kept secret.").

41. The Uniform Trade Secrets Act defines "reverse engineering" as "starting with the known product and working backward to find the method by which it was developed." GERALD B. HALT, JR. ET AL., INTELLECTUAL PROPERTY IN CONSUMER ELECTRONICS, SOFTWARE AND TECHNOLOGY STARTUPS 31 (2014).

42. *See id.* (identifying independent discovery as another defense to allegations of trade secret violations).

43. *See* Martijn Blaauw et al., *Privacy and Information Technology*, STAN. ENCYCLOPEDIA PHIL. (Edward N. Zalta ed., Spring 2016), http://plato.stanford.edu/archives/spr 2016/entries/it-privacy/ ("[R]ecent advances in information technology threaten privacy and have reduced the amount of control over personal data and open up the possibility of a range of negative consequences as a result of access to personal data.").

44. *See* David S. Levine, *supra* note 7, at 145-47 (discussing the theoretical framework of trade secrecy); WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 1 (2017) (arguing that privacy law will be proven to be capable of clear definition over the next decade).

45. Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

also untethered to any consistent theory,[46] and its necessity is often assumed without critical analysis. Therefore, like trade secrecy, the power of confidentiality and privacy as a generalized want or need can easily overwhelm the public's right to information, especially when the collective "we" fails to explain why it deserves access to otherwise "confidential" or "private" information—and no one asks the question.

This Article posits that the confidentiality creep, opportunistic privacy, and trade secrecy information access problems arise when we overlook *how* and *why* information is *used* and *needed* by the information's recipient. Trade secret doctrine is again instructive, as it suffers from this impediment largely because identifying the intended and actual *use* of trade secret information—the alleged misappropriation—is generally an overlooked and/or assumed aspect of trade secret law analysis.[47] Indeed, with the notable limited exception of the new Defend Trade Secret Act's whistleblower provision,[48] United States trade secrecy law has remained largely ignorant of the potential ill-effects of the secrecy it protects. But when we consider whether a given information request may lead to public benefits, we can more easily decide whether such information disclosure is worth the subsequent related harms, if any.

This issue has been raised in past scholarship. For example, I have identified and analyzed the dubious cabining of information, ranging from hydraulic fracturing's chemical formulas, to the code inside voting machines.[49] Invoking allegations of potential competitive disadvantage, I argued that trade secrecy has morphed into a shape-shifting doctrine that can create a safe harbor from public oversight and knowledge.[50] Additionally, Frank Pasquale's chapter in *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* focused on trade secret

---

46. *See generally* STEPHEN GILLERS, REGULATION OF LAWYERS: PROBLEMS OF LAW AND ETHICS 4 (10th ed. 2015) (discussing whether there should be a lawyer's confidentiality exception to protect others from a client's illegal conduct, and noting that "the conversation can go on and on, leading to broader and broader generalizations," because there is no single theory of confidentiality).

47. *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRET LAW, CASES AND MATERIALS 231-32 (2d ed. 2017) (identifying and explaining three separate trade secret misappropriation "wrongful actions: acquisition, disclosure, [and] use," and focusing on the "acquisition" action).

48. *See* 18 U.S.C. § 1833(b)(1)(A) (2012).

49. *See generally* David S. Levine, *Can We Trust Voting Machines?*, SLATE (Oct. 24, 2012, 7:52 AM), http://www.slate.com/articles/technology/future_tense/2012/10/trade_secret_law_makes_it_impossible_to_independently_verify_that_voting.html.

50. *See id.*; *see also* Levine, *supra* note 5.

protected search engine ranking systems.[51] Pasquale's subsequent groundbreaking book, *The Black Box Society: The Secret Algorithms that Control Money and Information*, extended that analysis to healthcare and credit scores.[52] Pasquale explained that trade secrecy is deployed to prevent understanding of what data is being considered and how such data is being utilized in decisionmaking processes.[53]

Finally, trade secrecy often operates in tandem with other controls on information flow, such as contracts, the threat of conversion and trespass to chattels, and even federal laws like the Computer Fraud and Abuse Act.[54] When these laws combine with other limitations to information access, like exemptions to the Freedom of Information Act,[55] attorney-client privilege claims,[56] homeland security laws on critical infrastructure,[57] overwhelmed regulators,[58] increasingly high pleading

---

51. *See generally* Frank Pasquale, *The Troubling Consequences of Trade Secret Protection of Search Engine Rankings*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 381, 381-405 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011).

52. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

53. *See id.*; *see also* Mitch Ambrose, *Senator Seeking Greater Transparency in Research Underpinning Regulations*, AM. INST. PHYSICS (Mar. 23, 2017), http://www.aip.org/fyi/2017/senator-seeking-greater-transparency-research-underpinning-regulations ("Sen. James Lankford (R-OK) has introduced a bill that would set standards for how federal agencies consider scientific findings when developing regulations" and the level of public access to such findings.).

54. *See generally* Computer Fraud and Abuse Act § 2, 18 U.S.C. § 1030 (2012); Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).

55. *See, e.g.*, Freedom of Information Act, 5 U.S.C. § 552(b)(4) (2012) (noting that the FOIA does not apply "to matters that are . . . trade secrets and commercial or financial information obtained from a person and privileged or confidential).

56. *What Are FOIA Exemptions?*, Listed in *Frequently Asked Questions*, FOIA.GOV, http://www.foia.gov/faq.html#exemptions (last visited Nov. 1, 2017) ("Congress established nine exemptions from disclosure for certain categories of information to protect against certain harms, such as an invasion of personal privacy, or harm to law enforcement investigations.").

57. For example, "Congress created the Protected Critical Infrastructure Information ('PCII') Program under the Critical Infrastructure Information ('CII') Act of 2002 to protect private sector infrastructure information voluntarily shared with the government for the purposes of homeland security." *Protected Critical Infrastructure Information (PCII) Program*, HOMELAND SECURITY (June 28, 2017), http://www.dhs.gov/pcii-program; *see also* 6 C.F.R. pt. 29 (2017) (establishing PCII's uniform procedures for receiving, validating, and handling information voluntarily submitted to the Department of Homeland Security).

58. For example, "overwhelmed regulators" of the Securities and Exchange Commission cut "the investment industry—and themselves—some slack" by providing "temporary relief" from the looming effective date of certain provisions of the Dodd-Frank Act. David S. Hizenrath, *Overwhelmed Regulators Give Financial Industry a Reprieve*, WASH. POST (June 10, 2011), http://www.washingtonpost.com/blogs/political-economy/post/overwhelmed-regulators-give-financial-industry-a-reprieve/2011/06/10/AGPiMnOH_blog.html?utm_term=.11ef030ff9ac. 59.

Per *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), the United States Supreme Court raised the pleading standard necessary for civil complaints to survive dismissal pursuant to Federal Rules of Civil Procedure 12(b)(6). However,

standards,[59] technical complexity,[60] and now confidentiality creep and opportunistic privacy, the combined effect becomes a "Ring of Gyges."[61] This figurative ring ends the very possibility of understanding new technologies and precludes accountability for destructive actions.

In sum, when viewed separately, an individual information control argument or law might be overcome. But when the above laws and limitations are combined, an often impenetrable wall of secrecy around given technologies can arise. While it is beyond the scope of this Article to assess all of the above doctrines and their ramifications, future scholarship will explore how and why these seemingly disparate laws and conditions combine to create massive and destructive technological information blindness, how this condition impacts professions like law and policymaking, and what we can do to analyze and address this problem.[62] For now, the more limited but nevertheless important focus is to identify the problem of losing the very ability to appreciate the strangeness in our midst through confidentiality creep and opportunistic privacy.

B. A Background Example: Hydraulic Fracturing Trade Secrets

Existing secret methods and processes have and are impacting the natural world in ways that we are just now beginning to understand. A good illustration of this lag-time problem, and the power of trade secrecy left unexamined, is the hydraulic fracturing chemical manufacturer Baker Hughes' position regarding its hydraulic fracturing trade secrets.[63] Hydraulic fracturing, or "fracking," is an oil and gas extraction technique that uses a fluid made from water, sand, and chemicals to crack rock

---

this higher pleading standard is limited to civil matters governed by the Federal Rules of Civil Procedure.

59. Per *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), the United States Supreme Court raised the pleading standard necessary for civil complaints to survive dismissal pursuant to Federal Rules of Civil Procedure 12(b)(6). However, this higher pleading standard is limited to civil matters governed by the Federal Rules of Civil Procedure.

60. *See* Felten, *supra* note 14 ("The second type of explainability problem is *complexity.* Here everything about the algorithm is known, but somebody feels that the algorithm is so complex that they cannot understand it.").

61. In Plato's *Republic*, the "Ring of Gyges" is a ring that renders whoever wears it invisible. *See* Andrew Laird, *Ringing the Changes on Gyges: Philosophy and the Formation of Fiction in Plato's Republic*, 121 J. HELLENIC STUD. 12, 12 (2001). Ideas in this paragraph derive from the prior unpublished project identified in the biographical footnote *supra*.

62. This is in the aforementioned *Public Data Science* project. *See supra* note 14.

63. *See Hydraulic Fracturing Chemical Disclosure Policy*, BAKER HUGHES, http://www.bakerhughes.com/products-and-services/pressure-pumping/hydraulic-fracturing/environmental-solutions-and-chemical-disclosure/disclosure (last visited Oct. 4, 2017).

containing fossil fuels and stimulate the flow of oil and gas to the surface.[64] Baker Hughes, which has been the most transparent of the hydraulic fracturing fluid manufacturers, explained that it "will provide a complete, detailed, and public listing of all chemical constituents for all wells that the company fractures using its hydraulic fracturing fluid products," but will not reveal "proprietary formulations" while advancing "commercial innovation, all of which are critical factors in our focus on ever more effective, efficient and sustainable hydraulic fracturing chemistry."[65]

The energy sector has asserted proprietary information protections for both its drilling methods and the chemicals used in hydraulic fracturing.[66] Indeed, the chemical formula used in hydraulic fracturing is not just a trade secret but could easily be identified as a paradigm trade secret, given the preponderance of trade secrecy as an appropriation method in the chemical industry.[67] Baker Hughes's use of trade secrecy to protect its formula from competitor misappropriation is a textbook example of how trade secrecy is designed to work.

However, there is a significant public cost to this protection. While there are economic benefits derived from hydraulic fracturing, including cheaper energy,[68] there are also environmental, health, and safety (EHS) risks associated with it.[69] Public access to and understanding of the formula is needed so as to understand and assess the precise risks borne by the public when a well is fractured and to assure the public that such activities do not unduly raise EHS risks.[70] Without such access, we are unable to precisely assess the likelihood and severity of EHS risks.

Perhaps counterintuitively, the understanding blind spot is not only problematic for the public, it can be problematic for the hydraulic

---

64. *See Hydraulic Fracturing 101*, EARTHWORKS, http://www.earthworksaction.org/issues/detail/hydraulic_fracturing_101#.WdU7eBNSxE4 (last visited Oct. 4, 2017).

65. *See Hydraulic Fracturing Chemical Disclosure Policy*, *supra* note 63.

66. *See* Alexis L. Maule, *Disclosure of Hydraulic Fracturing Fluid Chemical Additives: Analysis of Regulations*, 23 NEW SOLUTIONS 167, 169 (2013) ("Since companies invest time and resources into perfecting their fluid technologies, industry views chemical recipes as proprietary information that should be protected as trade secrets; thus many of the chemicals used remain unknown.")

67. *See* David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?* (unpublished draft article) (on file with author).

68. Fred Dews, *The Economic Benefits of Fracking*, BROOKINGS (Mar. 23, 2015), http://www.brookings.edu/blog/brookings-now/2015/03/23/the-economic-benefits-of-fracking/.

69. *See generally* David S. Levine & Mary L. Lyndon, Law Professors' Second Alaska Oil and Gas Conservation Commission Trade Secrets Letter (Oct. 14, 2013) (unpublished comment), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2363099.

70. *See id.*; *see also* Dave Cocchiarella, *Fracking's Secret Sauce*, FORWARD FLA. (Feb. 24, 2016), http://forwardflorida.com/energy/frackings-secret-sauce/.

fracturing industry itself. This condition was identified by former North Carolina Mining and Energy Commission (MEC) Chairman James Womack, who was assigned the task of drafting North Carolina's hydraulic fracturing regulations.[71] When confronted with strong lobbying by the chemical industry to create ironclad protections for chemical trade secrets, Womack saw that the resulting information vacuum could harm the hydraulic fracturing industry's interests. In a letter to the North Carolina Legislature, Womack explained that failing to share chemical trade secrets with the public would mean that "[c]itizens would be forced to rely on research by third party organizations opposed to shale gas exploitation."[72] In other words, in the public's search for information, trade secrecy would result in the hydraulic fracturing industry losing control of the narrative (and therefore public perception of hydraulic fracturing) to its environmental policy nemeses.[73]

An additional concern about trade secret designations in hydraulic fracturing activity is the "lag time" problem. Because today's activities can often only be measured and felt months, years, and even decades later, the impact of today's secrecy can have ramifications long after the entities that caused the harms disappear.[74] This possibility could effectively leave no one accountable for EHS harms. Moreover, this lag time creates a massive risk of environmental harm as problems develop imperceptivity and become difficult or impossible to mitigate once they are felt.[75]

---

71. The author served on the MEC as a member of the Trade Secrets Study Group, where he advised the MEC on how to draft its proposed regulations with regard to trade secrecy. While the language ultimately passed was not ideal, the author was able to raise his concerns in several public meetings.

72. Comm'r Jim Womack, N.C. Mining & Energy Comm'n, Comment Letter on Mining and Energy Commission Concerns with Chemical Disclosure and Trade Secret Modifications (June 30, 2013), http://www.smithenvironment.com/wp-content/uploads/2013/07/H94-Concerns_MEC-Memo_30Jun2013-1.pdf.

73. *See generally* ALISTER MISKIMMON, BEN O'LOUGHLIN & LAURA ROSELLE, FORGING THE WORLD: STRATEGIC NARRATIVES AND INTERNATIONAL RELATIONS (2017).

74. Those hydraulic fracturing chemical harms include

> significant environmental and human health risks. Many are toxic. A number are classified as known or probable carcinogens. These chemicals may be released into the environment in multiple ways. Fracking fluids have spilled, contaminating soil and water bodies. Equipment failures and other problems have led to well blowouts during fracking, spraying fracking fluids into the air and onto surrounding lands. Fracking also has the potential to cause groundwater contamination.

Matthew McFeeley, *Falling Through the Cracks: Public Information and the Patchwork of Hydraulic Fracturing Disclosure Laws*, 38 VT. L. REV. 849, 852 (2013).

75. *See The Environmental and Social Impacts of Natural Gas Fracking*, FORBES (Apr. 17, 2017, 11:51 AM), http://www.forbes.com/sites/quora/2017/04/17/the-environmental-and-

As a result, trade secrecy has morphed into a method to prevent public understanding of the costs borne by the public through hydraulic fracturing. Additionally, because regulators often have an interest in supporting the industries that they regulate,[76] no state has directly challenged the argument that trade secrecy is a necessary prerequisite to innovation.[77] While such challenges would be difficult to mount given the level of chemical industry knowledge that would be required, the EHS risks have historically been subsumed to trade secrecy's lure as a necessary prerequisite to progress.[78]

However, there is reason to believe that an evolution is beginning, which is led by Montana. Signed in May 2017, Montana State Bill 299[79] allows hydraulic fracturing chemical formula trade secrets to exist but creates a process of judicial review of the state administrative entity's determination of trade secret status.[80] Thus, at least in Montana, there appears to be recognition that the public may have a greater interest in access to trade secret information than previously acknowledged by law or policy. Nonetheless, as a general matter, and unless regulators are diligent in their policing of industry practices, the public will remain in the dark about the true extent of the EHS risks.

The hydraulic fracturing trade secret legislative example is instructive. Like today's technology battles, information remains captured by those with the incentive to keep it secret, and challenging the need for secrecy is difficult. In the case of hydraulic fracturing, those who know the EHS risks best may be the chemical companies

---

social-impacts-of-natural-gas-fracking/#522285b41a76 (describing the irreparable environmental harms of fracking).

76. *See generally 20th Century US Capitalism and Regulation*, KAHN ACAD., http://www.khanacademy.org/humanities/us-history/history-survey/us-history-survey/v/20th-century-capitalism-and-regulation-in-the-united-states (last visited Oct. 4, 2017).

77. *See* Vanessa Schipani, *The Facts on Fracking Chemical Disclosure*, FACTCHECK.ORG (Apr. 7, 2017), http://www.factcheck.org/2017/04/facts-fracking-chemical-disclosure/ ("Along with other regulations related to the practice, as of January 2016, 28 states require the disclosure of some, but not all, chemicals used during fracking. . . . But fracking operators don't have to report *all* the chemicals they use in part because of trade secrets laws . . . ."). The closest challenge that we have is Montana State Bill 299. *See* S.B. 299, 65th Leg., Reg. Sess. (Mont. 2017).

78. Levine & Lyndon, *supra* note 69 ("While businesses engaged in hydraulic fracturing may have legitimate trade secrets, the public's interest in assuring that hydraulic fracturing is managed in a manner that addresses all significant risks may legitimately outweigh commercial concerns.").

79. *See* Mont. S.B. 229.

80. Tyler J. Hall, *Full* Disclosure: A Middle Road in Fracking Fluid Law*, ORRICK (Mar. 9, 2017), http://blogs.orrick.com/trade-secrets-watch/2017/03/09/full-disclosure-a-middle-road-in-fracking-fluid-law/.

themselves, who have little incentive to be any more transparent than they are now, while public harms amass.

Google's and Uber's autonomous car information practices and the Russian Facebook influence campaign, discussed below in Section II.C, reflect a similar array of challenges, with confidentiality creep and opportunistic privacy taking center stage. While trade secrecy also plays a role, the arguments for keeping information from the public are more amorphous and ephemeral but no less urgent. Like hydraulic fracturing harms, we do not want to run the risk that by the time we figure out what we need to know, the technological harms (i.e., an election poisoned by a foreign misinformation campaign) will have already occurred. As it stands now, the law remains in an awkward position to help address this problem.

C. The Perfect Storm: Algorithms

Algorithms are similar to hydraulic fracturing trade secrets, as they play a critical but poorly understood role in our information ecosystem. Facebook, Google, Uber, and countless other entities use algorithmic operations to steer information flows, rank content, strategically place product ads, and predict future user behavior.[81] Moreover, while computers offer the allure of objectivity, algorithms are neither neutral, nor objective. Instead, they reflect the subjective interpretations and decisions of their human programmers, whose personal prisms of view can lead to unintended or intended discrimination.[82]

A common concern regarding algorithmic decision-making is the opaque nature of many algorithms. Algorithms are often practically inscrutable to the outside observers and can be difficult to comprehend, even if their source code was shared with competent observers.[83] This complexity adds to their power; however, algorithms that are complex and opaque can make it difficult to understand their processes or intervene in their operations and outcomes.

---

81. *See* Nizan Geslevich Packin & Yafit Lev-Aretz, *On Social Credit and the Right To Be Unnetworked*, COLUM. BUS. L. REV. 339, 361 (2016) (explaining that entities "generat[e] algorithm[s] around behavioral data gleaned from social media and social networking information").

82. *See* Danah Boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC'Y 662, 665 (2012) (explaining that algorithms can "extract and illustrate large-scale patterns in human behavior").

83. *See* PASQUALE, *supra* note 52, at 1; Kroll et al., *supra* note 28; Frank Pasquale, *Shadow of the Smart Machine: Professions in an Era of Algorithmic Power*, NESTA (Feb. 5, 2016), http://www.nesta.org.uk/blog/shadow-smart-machine-professions-era-algorithmic-power.

Because algorithms decide "which information is 'best', and how to measure it,"[84] we face a risk assessment similar to that of hydraulic fracturing trade secrets when they are foisted upon the public. Shouldn't the public have a right to understand how such algorithms lead to information access and secrecy, so as to assess the algorithm's apparent judgment? Moreover, if one's actions and experiences are to be increasingly defined by and mediated through algorithmic processes, we should be interested in establishing ways to hold these algorithmic systems accountable.[85]

Public understanding of online information platforms like Facebook and Google is further obscured by the fact that the underlying algorithms are frequently deployed invisibly. Indeed, like former Defense Secretary Rumsfeld's "unknown unknowns,"[86] users are often unaware of the algorithms' very existence.[87] Moreover, many algorithms are entirely opaque because their source code, principles of functioning, and basic operations are truly secret.[88] Indeed, it is wholly uncontroversial to designate algorithms as trade secrets—full stop.[89]

---

84. Marissa Mayer, *Do Not Neutralise the Web's Endless Search*, FIN. TIMES (July 14, 2010), http://www.ft.com/intl/cms/s/0/0458b1a4-8f78-11df-8df0-00144feab49a.html#axzz3ziVCVGRE.

85. In an article on the opacity of algorithms, Jenna Burrell discusses how to investigate opacity in algorithms with examples from actual coding processes and education. She distinguishes between different types of opacity, e.g., "opacity as technical illiteracy," "opacity as intentional corporate or state secrecy," and "opacity that arises from the characteristics of machine learning algorithms," and points to the complexity involved in investigating the opacity of machine learning algorithms and assessing their impact. The investigative method needed is manifold, she concludes:

> Ultimately partnerships between legal scholars, social scientists, domain experts, along with computer scientists may chip away at these challenging questions of fairness in classification in light of the barrier of opacity. Additionally, user populations and the general public can give voice to exclusions and forms of experienced discrimination (algorithmic or otherwise) that the "domain experts" may lack insight into. Alleviating problems of black boxed classification will not be accomplished by a single tool or process, but some combination of regulations or audits (of the code itself and, more importantly, of the algorithms functioning), the use of alternatives that are more transparent (i.e. open source), education of the general public as well as the sensitization of those bestowed with the power to write such consequential code. The particular combination of approaches will depend upon what a given application space requires.

See Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, BIG DATA & SOC'Y, Jan.-June 2016, at 1, 10.

86. *See* Rumsfeld Press Conference, *supra* note 31.

87. *See* Motahhare Eslami et al., *"I Always Assumed that I Wasn't Really that Close to [Her]": Reasoning About Invisible Algorithms in News Feeds*, PROCEEDINGS OF THE 33RD ANNUAL CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, Apr. 2015, at 153, 153.

88. *See* PASQUALE, *supra* note 52; Danielle Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 8980 WASH. L. REV. 1, 7 (2005) ("Although

1. Confidentiality Creep and Autonomous Cars

Still, we have seen the more amorphous and ill-defined confidentiality creep arise within the context of algorithmic disclosure. Perhaps the best example of its deployment is in the regulation of autonomous vehicles. Autonomous vehicles are generally defined as automobiles that operate, in whole or in part, without direct human control.[90] Instead, they operate via a complex web of technologies governed by algorithms.[91]

Autonomous cars, as they remain in their infancy, are tested on public roads. This reality creates massive questions regarding who should bear the risk of an accident.[92] But perhaps more fundamentally, this condition also raises questions about who should decide whether such tests should occur in public places (where the public bears the risk of errors) and whether and to what extent risks even exist.

In order to understand and answer these more complex questions, algorithms must be made accessible to the public. As explained succinctly by Patrick Lin with regard to the algorithms that decide whether an autonomous car will brake in order to avoid an accident:

> If the rationale behind these common decisions is not transparent, then we can't accurately judge the risk of these products as they drive on our streets, alongside our families and friends. Especially if these cars are still in "beta-testing mode"—if the kinks are still being ironed out—our *informed* consent is important in what's essentially a massive human-subjects experiment on whether two-plus tons of machinery can self-drive around moving people.[93]

To be sure, the "rationale" is governed by algorithms, as is our ability to provide "informed consent." Thus, Google's penchant for confidentiality creep with regard to data (generated by algorithm) accessibility is problematic. For example, in 2014, Google confronted the possibility of having to share "data related to 'disengagements'—

---

algorithmic predictions harm indiviuals' life opportunities often in arbitrary and discriminatory ways, they remain secret.").

89. 1 Shue, Vergari, State Computer Law § 3:130, Westlaw (database updated Aug. 2017) (explaining that an algorithm was undisputedly considered a trade secret).

90. *See* Harry Surden & Mary-Anne Williams, *Technological Opacity, Predictability, and Self-Driving Cars*, 38 CARDOZO L. REV. 121, 125 (2016) ("Autonomous or "self-driving" cars are computer-controlled vehicles, capable of driving on their own without being operated by a person.").

91. *Id.* at 141.

92. *Id.* at 147.

93. Patrick Lin, *Robot Cars and Fake Ethical Dilemmas*, FORBES (Apr. 3, 2017), http://www.forbes.com/sites/patricklin/2017/04/03/robot-cars-and-fake-ethical-dilemmas/#641972c113a2.

when the robotic car hands back control to its human test driver" with the California Department of Motor Vehicles (DMV).[94] The DMV wanted this data, which included "the location and weather conditions, to help it create driver tests for when autonomous vehicles eventually go on sale to the public."[95] In response, Google took the following position: "An overly broad reporting requirement will create a significant burden on manufacturers. But it will also create a *significant burden on DMV . . . and will pose a particular challenge since DMV does not have the existing engineering expertise to interpret the data*."[96]

This response demonstrates confidentiality creep in its purest form: Google preferred to withhold information for the amorphous reason that such information would not be understood. Put directly, there is no theoretical or policy-based rationale for keeping information confidential simply because the entity requesting the information may lack the expertise needed to understand it. Like the hydraulic fracturing trade secret example discussed above, one could argue that sharing such information would build capacity to understand within the DMV and the public itself, which would positively impact the public's perception of a technology often viewed as scary, out-of-control, and deadly.[97] The very perception of transparency may itself be beneficial to Google.

Nonetheless, Google's argument is powerful precisely because it is amorphous, as it is difficult to argue against that which lacks clear parameters. Additionally, it suggests that Google is tethered to the idea that it "knows best," missing the greater concern that the public has an interest in understanding new technologies, even if its progenitors are viewed as benevolent (as Google often is).[98] Thus, confidentiality creep reflects not only a potential practical challenge in policymaking, but perhaps more importantly, it is a direct attack on the notion that there is value for purposes of democratic accountability[99] in access to information more generally.

Uber, the online taxi service, enters the equation in a related way that bears noting. Because Uber has been allowed in cities like

---

94. Mark Harris, *These Are the Secrets Google Wanted To Keep About Its Self-Driving Cars*, QUARTZ (Aug. 21, 2014), http://qz.com/252817/these-are-the-secrets-google-wanted-to-keep-about-its-self-driving-cars/ (emphasis added).

95. *Id.*

96. *Id.* (emphasis added).

97. Kartik Hosanagar & Imran Cronk, *Why We Don't Trust Driverless Cars—Even When We Should*, HARV. BUS. REV. (Oct. 18, 2016), http://hbr.org/2016/10/why-we-dont-trust-driverless-cars-even-when-we-should.

98. Surden & Williams, *supra* note 90.

99. Siva Vaidhyanathan, *Facebook Wins, Democracy Loses*, N.Y. TIMES (Sept. 8, 2017), http://www.nytimes.com/2017/09/08/opinion/facebook-wins-democracy-loses.html.

Pittsburgh to unilaterally decide how and when to test its autonomous cars on public roads,[100] it has magnified confidentiality creep. Here is how *The New York Times* described the state of play days prior to Uber's September 2016 launch of driverless Uber cars:

> There have been no public service announcements or demonstrations of the technology. Except for the mayor and one police official, no other top city leader has seen a self-driving Uber vehicle operate up close. Fire and emergency services don't know where the Uber cars will travel.
>
> It is precisely this hands-off approach that has made Pittsburgh ideal grounds for one of Silicon Valley's boldest experiments—and it has ignited criticism that the city is giving away its keys to Uber, which is testing a nascent technology and has a reputation for running roughshod over regulators and municipalities.[101]

Thus, by acting without any pretense of the need to explain its decision-making, Uber has elevated confidentiality creep. From where did it derive the authority to act unilaterally and enable confidentiality creep? The answer lies in finding the unexplored "empty space" in our regulatory world, where there are no rules governing such a decision, and where those elected to create such rules and assure public safety and understanding do not perceive the need to act, leaving it to Uber to make the decision.

Of course, Uber was not acting illegally; indeed, it followed Pittsburgh's lead in allowing confidentiality to take hold by announcing its decision to start using driverless cars with customers just a few days before the September 2016 implementation date.[102] However, in the intervening months, Uber's secrecy and lack of corporate accountability predictably led to a deterioration of the city's relationship with Uber.[103] As reported in May 2017 by *The New York Times*, "Uber said it planned to share some data collected by its autonomous vehicles with the city this year, though Pittsburgh officials say the data Uber shares with other cities is insufficient."[104] More recently, a spokesperson for "the Self-Driving Coalition for Safer Streets, which includes Ford, Alphabet's Waymo, Volvo Cars, Uber and Lyft, said the companies would oppose

---

100. Cecilia Kang, *No Driver? Bring It On. How Pittsburgh Became Uber's Testing Ground*, N.Y. TIMES (Sept. 10, 2016), http://www.nytimes.com/2016/09/11/technology/no-driver-bring-it-on-how-pittsburgh-became-ubers-testing-ground.html.

101. *Id.*

102. *Id.*

103. Cecilia Kang, *Pittsburgh Welcomed Uber's Driverless Car Experiment. Not Anymore.*, N.Y. TIMES (May 21, 2017), http://www.nytimes.com/2017/05/21/technology/pittsburgh-ubers-driverless-car-experiment.html?mcubz=1.

104. *Id.*

broad data disclosure requirements," citing privacy and trade secret concerns.[105]

As it stands today, Google and Uber's general position with regard to confidentiality remains highly relevant. The National Highway Traffic Safety Administration (NHTSA) is the primary entity now considering safety requirements for autonomous vehicles.[106] As *The Washington Post* recently reported, the NHTSA is currently taking a "hands-off" approach to safety regulations, as "[t]he guidelines continue to rely on technology companies and automakers to voluntarily submit information explaining why their cars are safe and how their passengers will be protected."[107] While there is a bill in Congress that would set more exacting standards, it remains under debate and still protects companies from robust disclosure obligations.[108]

Therefore, even if the bill were to become law, control of the national discussion around algorithmic accountability and autonomous cars appears to remain at the hands of the autonomous car manufacturers themselves.[109] As with hydraulic fracturing trade secrets, the propensity to assume that confidentiality is needed, with no reason to explain or substantiate such a designation of seemingly private information, renders amorphous confidentiality claims powerful.

Thus, we must guard against confidentiality creep becoming an easy way to prevent public understanding, and therefore open analysis and discussion of the integration of autonomous cars into society. Opportunistic privacy is at play here, as well, but it is more easily identified by examining Facebook's handling of the purchase of political content by Russian interests leading up to the 2016 presidential election. Opportunistic privacy is discussed below.

---

105. Reuters, *U.S. Push for Self-Driving Law Uncovers a Regulatory Divide*, JAPAN NEWS (Sept. 17, 2017, 8:06 PM), http://the-japan-news.com/news/article/0003945834.

106. *NHSTA Releases Self-Driving Car Guidelines*, BUS. INSIDER (Sep. 21, 2016), http://www.businessinsider.com/nhtsa-releases-self-driving-car-guidelines-2016-9.

107. Michael Laris, *Updated Federal Driverless Policy Continues, and Expands, Hands-Off Approach*, WASH. POST (Sept. 12, 2017), http://www.washingtonpost.com/local/trafficandcommuting/updated-federal-driverless-policy-continues-and-expands-hands-off-approach/2017/09/12/7db413fc-97c9-11e7-82e4-f1076f6d6152_story.html?utm_term=.1c8f9c58d0eb.

108. Aarian Marshall, *Congress United (Gasp) To Spread Self-Driving Cars Across America*, WIRED (Sept. 6, 2017, 4:00 PM), http://www.wired.com/story/congress-self-driving-car-law-bill/.

109. Laris, *supra* note 107 ("Earlier this year, California officials proposed requiring that companies provide them with copies of the voluntary letters the firms submit to NHTSA. A NHTSA official said it is 'a much cleaner and streamlined approach' to make companies responsible for releasing their own letters, rather than having them come through federal safety officials, which left the mistaken impression their content had to be approved in Washington.").

2. Social Media and Opportunistic Privacy

Algorithms, like Google's search functions and Facebook's posting of user content, decide what information gets attention, is ignored, gets published, and is censored.[110] Search engines function as gatekeepers[111] and influence the information that individuals get about the world. Social media uses similar algorithmic processes to decide what content to display to its over 2 billion customers[112] and when to display it.[113]

These algorithms operate within the limits of human capacity to write code but, once released, can operate independent of their programmers.[114] As a result, they can operate in unpredictable ways. For example, Goldman,[115] Mager,[116] and Bozdag[117] describe the many forms of

---

110. *See*, *e.g.*, James Grimmelmann, *The Google Dilemma*, 53 N.Y.L. SCH. L. REV. 939 (2008) (explaining that while whoever controls the search engines likely controls the Internet, itself, "no one comes closer to controlling search than Google does"); Joshua G. Hazan, *Stop Being Evil: A Proposal for Unbiased Google Search*, 111 MICH. L. REV. 789 (2013) (exploring Google's role within the greater Internet ecosystem and weighing the potential consequences of "Google hard-coding its own services at the top of the results page."); Julia Powles & Enrique Chaparro, *How Google Determined Our Right To Be Forgotten*, GUARDIAN (Feb. 18, 2015), http://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search (detailing the rights of individuals with regard to private—and sometimes inaccurate—personal information made public by websites like Google).

111. *See*, *e.g.*, Laura A. Granka, *The Politics of Search: A Decade Retrospective*, 26 INFO. SOC'Y 364 (2010) (describing the thought behind search engine regulation, online diversity, and information, and examining these issues in the context of technical and societal changes in the online search industry); Lucas D. Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16 INFO. SOC'Y 169 (2000) (arguing that search engines raise not only technical issues but also *political* ones).

112. *The Top 20 Valuable Facebook Statistics—Updated October 2017*, ZEPHORIA, http://zephoria.com/top-15-valuable-facebook-statistics/ (last updated Oct. 18, 2017).

113. AJ Agrawal, *What Do Social Media Algorithms Mean for You?*, FORBES (Apr. 20, 2016), http://www.forbes.com/sites/ajagrawal/2016/04/20/what-do-social-media-algorithms-mean-for-you/#6a7d425fa515.

114. Ben Schiller, *Algorithms Control Our Lives: Are They Benevolent Rulers or Evil Dictators?*, FAST COMPANY (Feb. 21, 2017), http://www.fastcompany.com/3068167/algorithms-control-our-lives-are-they-benevolent-rulers-or-evil-dictators ("Sets of instructions for completing tasks or solving problems, algorithms are the governing principles of our age—the underlying equations that help us make decisions, and, in some cases, make decisions for us.").

115. *See* Eric Goldman, *Revisiting Search Engine Bias*, 38 WM. MITCHELL L. REV. 96, 101-02, 108-09 (2011) (arguing that "truly 'neutral' perspectives about search engine bias are increasingly rare" and that such "bias could create serious issues for online information credibility and accessibility").

116. *See* Astrid Mager, *Algorithmic Ideology*, 15 INFO. COMM. & SOC'Y 769, 772 (2012) ("[C]ritics have started to scrutinize the multi-faceted impact Google and other search engines have on our culture and economy." Consumer profiling, in particular, has been identified as a major criticism, as it enables search engines to adjust advertisements to users' own individual interests.).

117. *See* Engin Bozdag, *Bias in Algorithmic Filtering and Personalization*, 15 ETHICS & INFO. TECH. 209 (2013) (noting that by exercising bias toward an advertiser, a search engine necessarily limits "the diversity and democracy inherent to the information").

bias that can emerge from search engine code, from encouraging competition to creating information echo chambers.[118] As a result, users only see links from the same sources, only see posts from the same friends, and only get ads from the same brands. The result is an information "echo chamber" that reinforces personal beliefs and biases, rather than informing or challenging them.

Indeed, bias and values coding in algorithms exist independent of any intention to do harm. With regard to scoring algorithms, Citron and Pasquale stress that "[t]he biases and values of system developers and software programmers are embedded into each and every step of development."[119] Barocas and Selbst's groundbreaking analysis of discrimination in algorithmic decision-making explains that algorithmic decision procedures can "reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society. It can even have the perverse result of exacerbating existing inequalities by suggesting that historically disadvantaged groups actually deserve less favorable treatment."[120] Thus, as algorithms become increasingly embedded in previously human-influenced tasks, like information sorting and dissemination, there are secret biases and channels for which no full public accounting is possible—absent disclosure of the algorithms themselves.

One of the most obviously complex and opaque algorithms is Facebook's newsfeed.[121] Despite its considerable reach and everyday engagement, it remains opaque to all of its users, and its effects are likely complex to predict.[122] Some have experimented with the function and

---

118. Mager explicitly sees dominant capitalist values becoming embedded in the search results. *See* Mager, *supra* note 116, at 775-78. Goldman, on the other hand, addresses the issue of portalization: where Google previously wanted to refer users to third-party websites, it increasingly wants to do more, such as giving aggregated information, or it wants to provide more, such as mail, videos, images etc. The more it can assume a portal function, the more data it has for building prediction models. *See* Goldman, *supra* note 115, at 103-05. Bozdag identifies several issues with algorithmic systems. *See* Bozdag, *supra* note 117. A role traditionally reserved for journalists, machines are now in charge of filtering out "unimportant" information. *See id.* at 210-13. Because of this, people do not see different information on different days from different people, like you might while reading a newspaper or following a more traditional news source. *See id.* Instead, users are caught in a kind of "monoculture." *See id.*

119. Citron & Pasquale, *supra* note 88.

120. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 674 (2016).

121. *See* Eslami et al., *supra* note 87.

122. *Id. But see* Erin Griffith, *Facebook Can Absolutely Control Its Algorithm*, WIRED (Sept. 26, 2017, 3:14 PM), http://www.wired.com/story/facebook-can-absolutely-control-its-algorithm/ ("Facebook has repeatedly shown it can police content on its platform, particularly when doing so affects its $27 billion business. 'We're just a platform' is a convenient way to avoid taking full responsibility for an increasingly serious set of problems.").

behavior that influences the Facebook newsfeed algorithm just to see what it might do.[123] Nonetheless, because of its complexity, it is practically inscrutable to outside observers, even though it inevitably has values, biases, and potential discrimination coded into it.

This reality is especially concerning given recent evidence of secret efforts by the Russian government to influence the outcome of the 2016 presidential election in favor of President Donald Trump.[124] As has been widely reported, Russia engaged in a sophisticated effort to influence the outcome of the election by purchasing at least $100,000 worth of advertisements involving divisive political issues, from immigration to race relations, designed to influence voters in unknown ways.[125] Shockingly, *The Washington Post* reports that Facebook now believes that "126 million of its users may have seen content produced and circulated by Russian operatives, many times more than the company had previously disclosed about the reach of the online influence campaign targeting American voters."[126] The fact that even Facebook itself apparently has difficulty ascertaining the breadth of its content diffusion only highlights the massive disadvantage that regulators and the public have in ascertaining Facebook's power and impact as a speech platform.[127]

---

123. *See*, *e.g.*, Mat Honan, *I Liked Everything I Saw on Facebook for Two Days. Here's What It Did to Me*, WIRED (Aug. 11, 2014, 6:30 AM), http://www.wired.com/2014/08/i-liked-everything-i-saw-on-facebook-for-two-days-heres-what-it-did-to-me/ (explaining how *Facebook* uses algorithms to decide the content that shows up in an individual's "feed"); Elan Morgan, *I Quit Liking Things on Facebook for Two Weeks. Here's How It Changed My View of Humanity*, MEDIUM (Aug. 13, 2014), http://medium.com/swlh/i-quit-liking-things-on-facebook-for-two-weeks-heres-how-it-changed-my-view-of-humanity-29b5102abace#.xz1ao4i7p (detailing how the *Facebook* user experience changes once the user stops feeding its engine with "likes").

124. Nicole Perlroth, Michael Wines & Matthew Rosenberg, *Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny*, N.Y. TIMES (Sept. 1, 2017), http://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=stream&module=stream_unit&version=latest&contentPlacement=16&pgtype=collection. As explained by Ashkan Soltani, "Facebook[]'s newsfeed [is] fueled by engagement and outrage—making [it] susceptible to manipulation." Ashkan Soltani (@ashk4n), TWITTER (Oct. 30, 2017, 3:44 PM), http://twitter.com/ashk4n/status/925131208085815296.

125. Scott Shane & Vindu Goel, *Fake Russian Facebook Accounts Bought $100,000 in Political Ads*, N.Y. TIMES (Sept. 6, 2017), http://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html.

126. Craig Timberg & Elizabeth Dwoskin, *Russian Content on Facebook, Google and Twitter Reached Far More Users than Companies First Disclosed, Congressional Testimony Says*, WASH. POST (Oct. 30, 2017), http://www.washingtonpost.com/business/technology/2017/10/30/4509587e-bd84-11e7-97d9-bdab5a0ab381_story.html?utm_term=.6e4be3f540c8.

127. *Id.* A previous estimate indicated that although unknown due to the aforementioned secrecy of Facebook's algorithm and other factors, $100,000 would result in "reaching 3 million to 5 million people in a general audience, with that average person getting the same ad five times." Michelle Castillo, *$100,000 in Russian-Bought Facebook Ads Could Have Reached*

Therefore, Congress, public interest groups, and Facebook itself are investigating the role that Facebook played, if any, in the election outcome.[128] Under intense public and congressional pressure, Facebook recently agreed to share the content of these ads with Congress and implement a new advertising transparency policy.[129] Although most of these ads have yet to be made public (and may never be made public if opportunistic privacy takes hold), information is being reported to suggest that Russia bought ads that backed Democratic candidates Jill Stein and Bernie Sanders,[130] "exploit[ed] . . . racial . . . divisions,"[131] and even impersonated the real group United Muslims of America, all the while "simultaneously using other accounts to hawk virulently Islamophobic messages to right-wing audiences on Facebook."[132]

Until recently, however, Facebook denied that it played any role at all or that it had an issue to address.[133] However, as pressure mounted for it to act, Facebook suddenly changed course.[134] The Electronic Privacy Information Center's (EPIC) Marc Rotenberg succinctly explained the issue and interests at stake:

> Facebook admitted that it sold more than 3,000 ads to the "Internet Research Agency," a troll farm that spreads propaganda in support of Russian President Vladimir Putin and his allies and goes after his enemies. Political ads on most U.S. media are required to state their sources and funding. But the Russian troll farm hid behind Facebook's anonymous

---

Millions of Voters, CNBC (Sept. 29, 2017, 12:06 PM), http://www.cnbc.com/2017/09/29/russian-facebook-ads-how-many-people-could-you-reach-with-100000.html.

128. Scott Shane & Mike Isaac, *Facebook To Turn Over Russian-Linked Ads to Congress*, N.Y. TIMES (Sept. 21, 2017), http://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html.

129. *Id.*; *see also supra* notes 11-12 and accompanying text.

130. Josh Dawsey, *Russian-Funded Facebook Ads Backed Stein, Sanders and Trump*, POLITICO (Sept. 26, 2017, 9:03 PM), http://www.politico.com/story/2017/09/26/facebook-russia-trump-sanders-stein-243172.

131. Adam Entous, Craig Timberg & Elizabeth Dwoskin, *Russian Operatives Used Facebook Ads To Exploit America's Racial and Religious Divisions*, WASH. POST (Sept. 25, 2017), http://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html?utm_term=.53d7e2b0ba51.

132. Ben Collins, Kevin Poulsen & Spencer Ackerman, *Exclusive: Russians Impersonated Real American Muslims To Stir Chaos on Facebook and Instagram*, DAILY BEAST (Sept. 27, 2017, 4:29 PM), http://www.thedailybeast.com/exclusive-russians-impersonated-real-american-muslims-to-stir-chaos-on-facebook-and-instagram.

133. *Zuckerberg Denies Fake News on Facebook Had Impact on the Election*, NPR (Nov. 11, 2016), http://www.npr.org/sections/alltechconsidered/2016/11/11/501743684/zuckerberg-denies-fake-news-on-facebook-had-impact-on-the-election.

134. *See supra* note 88 and accompanying text.

> algorithms—a practice that would have violated the law had it been done in print or on television.[135]

It is here where opportunistic privacy arises as an impediment to information access. As Facebook states directly on its "Privacy Basics" page, "[y]ou have control over who sees what you share on Facebook. That way, you're free to express yourself the way you want."[136] Because Facebook wants to encourage its customers to share content and has legitimate interests in maintaining the privacy of its customers, it does not differentiate between Aunt Mary's hypothetical privacy interests in posting her picture of her dog Fluffy and Vladimir Putin's interest in suggesting that Hillary Clinton played a role in the rise of the Islamic State terrorist group.[137]

Facebook's privacy position, of course, does not address how to handle Facebook as a tool of foreign influence over a presidential election or cyberwarfare. Because of the aforementioned amorphous nature of privacy as a right, it is difficult to even make counterarguments that address the countervailing national security and democracy interests at stake or that address exactly why privacy should be subsumed in this case. Therefore, when Facebook initially refused to offer any information that could help the public understand whether it was fooled by a hostile foreign power when it voted for the U.S. President, it could rely on amorphous privacy arguments as its principled basis.[138]

---

135. Mark Rotenberg, *Facebook's Privacy Hokey-Pokey*, FORTUNE (Sept. 22, 2017), http://fortune.com/2017/09/22/facebook-russian-ads-fake-news-zuckerberg/.

136. *See Privacy Basics*, FACEBOOK, http://www.facebook.com/about/basics (last visited Sept. 30, 2017).

137. Erica Pandey, *Russians Posed as American Muslims on Facebook*, AXIOS (Sept. 27, 2017), http://www.axios.com/russians-posed-as-american-muslims-on-social-media-2490308764.html.

138. Dawsey, *supra* note 130. The debate over whether the Stored Communication Act (SCA) limits Facebook's ability to share information further underscores the risk that opportunistic privacy can be utilized in order to avoid regulatory oversight. As recently explained by EPIC's Alan Butler, the SCA "was enacted to protect the privacy of customers and subscribers of digital platforms (e.g., Facebook users). The law was not intended to shield advertisers or the platforms themselves from oversight, or to limit users' access to information about the communications they receive." Ryan Goodman, *Top Experts: Can Facebook Legally Disclose Russian Ads—What Does the Stored Communications Act Say?*, JUST SECURITY (Oct. 27, 2017, 10:32 AM), http://www.justsecurity.org/46347/expert-views-facebook-legally-disclose-russian-ads-stored-communications-act-1986/. Nonetheless, others argue that advertisements "have long been considered private data on par with email content and other records that the government must have a search warrant to obtain." *See* Timberg et al., *supra* note 11. The complexity opens the door wider for opportunistic use of a privacy shield on public disclosure of information that does not serve the pecuniary or reputational interests of the organization holding the information.

It says much about the merit of this position that EPIC's Rotenberg took a dim view of Facebook's position:

> Less than a week after the company was in California opposing a law to protect online privacy, Facebook was in Washington saying it could not reveal information about Russian interference with the election because of privacy laws. And then this week it decided it could cooperate with investigators. Talk about a change in privacy settings!
>
> As a privacy advocate, I normally stand up for companies that stand up for user privacy. In the hi-tech world, we need these firms to oppose broad government requests for personal data and to build strong privacy safeguards into their products. But Facebook is not protecting the privacy of its users when it stonewalls the public about the role of Russia in the 2016 election. Instead, it is hiding its business practices—and that's a problem.[139]

In other words, Facebook is engaging in opportunistic privacy: it is using amorphous privacy concerns in order to prevent access to its proprietary information, like its algorithms, that it would rather not share with the public. Privacy law is not equipped to deal with such a conflation of goals, but like trade secrecy, privacy's amorphous nature makes it prone to such abuses. Indeed, again like the hydraulic fracturing trade secrets example discussed above, Facebook may slowly recognize that it is better off by sharing algorithmic information with the public so as to not be perceived as aloof to the impact of its platform on world events (a description that its critics would like to cement).[140]

Still, even in the midst of, as National Public Radio put it, "users—some of them demonstrably Russian, others not—[trying] to use Facebook, Twitter and other platforms to jam a crowbar into existing American political divisions and wrench them further apart,"[141] opportunistic privacy exists to stymie efforts to prevent the next misinformation campaign, whether waged by Russia or any other entity hell-bent on destroying U.S. democracy. As this Article goes to publication at a dynamic time in algorithmic computing, only time will tell how Google, Facebook, Uber, and other entities that utilize powerful algorithmic systems, respond to the growing regulatory and public desire to understand and trust complex technologies unwittingly imposed upon the public. Because of their varying positive and negative effects, the

---

139. Rotenberg, *supra* note 135.

140. *See* Griffith, *supra* note 122.

141. Philip Ewing, *As Scrutiny of Social Networks Grows, Influence Attacks Continue in Real Time*, NPR (Sept. 28, 2017, 5:01 AM ET), http://www.npr.org/2017/09/28/554024047/as-scrutiny-of-social-networks-grows-influence-attacks-continue-in-real-time.

coming years will test the public's willingness to accept new technologies on faith and uncritically.

III. CONCLUSION

Lack of transparency raises important questions about public accountability, especially in an era where hostile foreign powers seek to secretly alter the outcome of domestic elections through misinformation campaigns. Whenever secret algorithms make inherently subjective decisions, we wonder how we might predict and address the next decision. If an algorithm is opaque, it becomes impossible for the public to understand the rationale behind any particular outcome or determine if, when, and how algorithms are misused.

Therefore, Stephan Noller has argued that transparency "is one of the most important principles when it comes to throwing light on the chaos."[142] Noller goes a step further and demands publishing algorithms' source codes as well as the data they use.[143] The AI Now Institute at New York University, in its report entitled *The 10 Top Recommendations for the AI Field in 2017*, recommends that "[c]ore public agencies, such as those responsible for criminal justice, healthcare, welfare, and education (e.g 'high stakes' domains) should no longer use 'black box' AI and algorithmic systems"; indeed, it is their number one recommendation.[144]

However, access to algorithms, like access to trade secrets, is not always an accountability panacea. Public access to an algorithm's source code does not guarantee that the public will have the resources and knowledge needed in order to understand it, scrutinize it, or even care. If there is a lack of alternative services, transparency may not lead to any noticeable differences in consumer behavior. Of course, there are also costs associated with disclosure, including the real possibility that new

---

142. Stephan Noller, *Why We Need an Algorithm Ethic*, GUARDIAN (Jan. 22, 2013), http://www.theguardian.com/media-network/media-network-blog/2013/jan/22/algorithm-ethic-mechanisms-control-security.

143. *Id.*

144. AI Now Institute, *The 10 Top Recommendations for the AI Field in 2017*, MEDIUM (Oct. 18, 2017), http://medium.com/@AINowInstitute/the-10-top-recommendations-for-the-ai-field-in-2017-b3253624a7. While beyond the scope of this Article, Facebook's experimentation with AI underscores the fact that we do not have a solid grasp on how AI could impact our world, or whether we would know what it was doing, even if it was. Recently, Facebook reported that "[w]hile developing negotiating chatbot agents, researchers at the Facebook Artificial Intelligence Research (FAIR) lab noticed . . . that the artificially intelligent (AI) bots had spontaneously developed their own non-human language." Karla Lant, *Facebook's Language-Creating AI Bots Are Now Required To Negotiate in English*, FUTURISM (July 31, 2017), http://futurism.com/facebooks-language-creating-ai-bots-are-now-required-to-negotiate-in-english/.

and innovative technologies remain "on the shelf" due to the lack of proper protection of the inventor's interest in profits.

Moreover, even if the details of a specific algorithm are accessible and the necessary technical expertise to investigate is available, hardcoded bias or discrimination may not be readily found. As explained by Tarleton Gillespie, algorithms do not function as standalone boxes, but as networked "sociotechnical assemblages" that include a multitude of human and non-human actors, with people debating models, setting target goals, cleaning training data, adjusting parameters, and choosing the specific context of application.[145] Thus, contextual and relational information is needed to fully assess an algorithm's function and impact.[146]

Therefore, it has been suggested that transparency is required at multiple dimensions of algorithmic decision-making.[147] In other words, our algorithmic transparency goal should be to enable the ability to explain how any particular outcome was produced. Understandably, some researchers and academics argue that it makes more sense to design systems from the start in a more considered and discrimination-

---

145. *See* Tarleton Gillespie, *Algorithm*, CULTURE DIGITALLY (June 5, 2014), http://culture digitally.org/2014/06/algorithm-draft-digitalkeyword/.

146. Courts are beginning to recognize the need for algorithmic information in order to assess arguments regarding constitutional rights depravations. In a 2016 decision by the Maryland Court of Special Appeals, due process rights in search and seizure involving the technology known as "Stingray" was under consideration. Faced with an information deficit due to confidentiality agreements and claims, the court articulated the need for more technological information and understanding:

> We observe that such an extensive prohibition on disclosure of information to the court . . . prevents the court from exercising its fundamental duties under the Constitution. To undertake the Fourth Amendment analysis and ascertain "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security," [*Terry v. Ohio*], it is self-evident that the court must understand why and how the search is to be conducted. . . . The analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use. A nondisclosure agreement that prevents law enforcement from providing details sufficient to assure the court that a novel method of conducting a search is a reasonable intrusion . . . obstructs the court's ability to make the necessary constitutional *appraisal*.

Maryland v. Andrews, 134 A.3d 324, 338-39 (Md. Ct. Spec. App. 2016) (emphasis added and omitted).

147. *See, e.g.*, Rachel Shadoan, *Why Algorithm Transparency Is Vital to the Future of Thinking*, AKASHIC LABS (July 11, 2014), http://www.akashiclabs.com/why-algorithm-transparency-is-vital-to-the-future-of-thinking/ (arguing that good documentation of algorithms is *necessary* for transparency, but not *sufficient*). For a groundbreaking and brilliant analysis of the ethics that should be associated with creating technologies, see Shannon Vallor's book, *Technology and the Virtues* (2016).

conscious way,[148] while legal scholars argue for the creation of new regulations or even regulatory bodies to govern the algorithms that make increasingly important decisions in our lives.[149]

In order to bring us closer to the ability of understanding how technology is integrated into our lives, we need to identify the role of confidentiality creep and opportunistic privacy and to recognize the differences between justified and dubious confidentiality and privacy claims. My future scholarship will explore theoretical and practical contours within the broader context of a call for a new field called "public data science."[150] For now, it suffices to merely isolate and scrutinize these two amorphous claims to information control that keep us from perceiving the strangeness in our midst.

148. *See* FAT/ML, http://www.fatml.org/ (last visited Oct. 27, 2017); CAMPAIGN TO STOP KILLER ROBOTS, http://www.stopkillerrobots.org/ (last visited Oct. 27, 2017); *see also* Kroll et al., *supra* note 28.

149. *See*, *e.g.*, PASQUALE, *supra* note 52; Danielle Keats Citron, *Big Data Should Be Regulated by 'Technological Due Process,'* N.Y. TIMES (July 29, 2016, 4:34 PM), http://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/big-data-should-be-regulated-by-technological-due-process (arguing that "all predictive systems should be subject to fairness requirements that reflect their centrality in people's lives"); Frank Pasquale, *Digital Star Chamber*, AEON (Aug. 18, 2015), http://aeon.co/essays/judge-jury-and-executioner-the-unaccountable-algorithm (explaining that cyberspace "is now a force governing [the 'real world'] via algorithms: recipe-like sets of instructions to solve programs . . . . [W]hen algorithms start affecting critical opportunities for employment, career advancement, health, credit and education, they deserve more scrutiny.").

150. *See* Claire Cain Miller, *Data Science: The Numbers of Our Lives*, N.Y. TIMES (Apr. 11, 2013), http://www.nytimes.com/2013/04/14/education/edlife/universities-offer-courses-in-a-hot-new-field-data-science.html.