Boston College Law School
Digital Commons @ Boston College Law School

Boston College Law School Faculty Papers

6-10-2020

Revisiting the Western Frontier

Alfred C. Yen
Boston College Law School, alfred.yen@bc.edu

Follow this and additional works at: https://lawdigitalcommons.bc.edu/lsfp

 Part of the Internet Law Commons, and the Legal Writing and Research Commons

Recommended Citation

Alfred C. Yen. "Revisiting the Western Frontier." *IDEA* 60, no.1 (2020): 134-148.

This Article is brought to you for free and open access by Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law School Faculty Papers by an authorized administrator of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.

REVISITING THE WESTERN FRONTIER

ALFRED C. YEN*

I appreciate very much the opportunity to look back on "old" scholarship. Hindsight is indeed 20/20, and there are things one could have done differently. Whether it would have been reasonably possible for me to do these things is an open question. Accordingly, I will divide my retrospective into three parts. In Part I, I will briefly summarize my work. Then, in Part II, I will discuss the things I wish I had included. Finally, in Part III, I will conclude with a few brief thoughts about what was reasonably possible at the time.

I. Disrupting Cyberspace as the Western Frontier 135
II. Taking Stock 137
A. The Extent of the Cybermanor..... 137
B. The Extent of Political Power 141
C. Who or What is the True Emerging Cyberlord? . 145
III. Conclusion 147

* Professor of Law and Dean's Distinguished Scholar, Boston College Law School.

I. DISRUPTING CYBERSPACE AS THE WESTERN FRONTIER

The work I have chosen to review is *Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace.*[1] I published this article in 2002 as a reaction to the then popular idea that the Internet was a libertarian utopia whose natural qualities made government regulation unnecessary or perhaps even harmful.[2] Among other things, proponents of this idea compared cyberspace to America's western frontier. This comparison adopted Frederick Jackson Turner's Western Frontier Thesis, which maintained that the frontier's abundant land and the simple lives of its inhabitants fostered uniquely American virtues responsible for the country's success.[3] Thus, to proponents of a digital utopia, cyberspace was just like the western frontier, or even better. And because the supposed lack of government regulation helped the frontier flourish, the same should go for the Internet.[4]

My article criticized the metaphorical comparison of the Internet as a western frontier in two ways. First, it observed that the comparison did not use an accurate

---

[1] Alfred C. Yen, *Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace,* 17 BERKELEY TECH. L.J. 1207 (2002).

[2] *See id.* at 1211–12 (identifying the argument that society should accept the Internet "as is" and avoid regulating the activities of those using the Internet).

[3] Frederick Jackson Turner, THE FRONTIER IN AMERICAN HISTORY 1–38 (Henry Holt & Co., 1st ed. 1920) ("American social development has been continually beginning over again on the frontier. This perennial rebirth, this fluidity of American life, this expansion westward with its new opportunities, its continuous touch with the simplicity of primitive society, furnish the forces dominating the American character. The true point of view in the history of this nation is not the Atlantic coast, it is the Great West.").

[4] *See* Yen, *supra* note 1, at 1226–29.

depiction of the western frontier, instead opting for a romanticized version of the west that whitewashed its flaws.[5] The unspoiled, simple American frontier that rewarded basic virtues while naturally defeating evil is really a romanticized vision adapted by popular culture.[6] Of course, movies make a much stronger impression on our collective imagination than historical texts do, so the romanticized frontier is quickly recalled and accepted as true. This overlooks the western frontier's tragic history of genocide, violence, and lawlessness. Thus, I argued that the case for Internet non-regulation could not rest on metaphorical comparison to a western frontier that never existed, especially when the real western frontier worked in a very different way.[7]

Second, the article offered feudalism as an alternate metaphor through which to view the Internet.[8] I made the claim that the Internet looked more like a world of developing feudal estates than a utopian western frontier. The Internet had a hierarchical structure derived from the domain name system.[9] Physical and political control over the Internet and its users became the consequences of private property on the Internet.[10] And, perhaps most importantly, the cyberlord owners of the Internet's feudal estates controlled and exploited their cyberserf users.[11] Although in theory these cyberserfs could try to escape, practical realities often stopped them from doing so, effectively binding cyberserfs to the estates of the feudal

---

[5] *See id.* at 1216–22, 1229–32.
[6] *See id.*
[7] *See id.* at 1229–32.
[8] *Id.* at 1243.
[9] *See id.* at 1237–39.
[10] *See id.* at 1239–48.
[11] *See id.* at 1243–48.

lords.[12] The deployment of a feudal metaphor disrupted the overly optimistic metaphor of the western frontier, turning the Internet from a place with unlimited freedom and opportunity into a place of oppression and exploitation. I argued that, to the extent that we object to living in a feudal society, legal regulation from the modern state was at least partly responsible for feudalism's demise. Thus, if we considered that a good development in the world, perhaps the imposition of some regulation on the Internet would be desirable.[13]

II. TAKING STOCK

Looking back on the article, I think the general direction was correct. It is pretty clear that the Internet did not become the libertarian utopia that some imagined. Indeed, it seems to me that although the Internet embodies many amazing things that improve modern life, those benefits come with significant costs related to the exploitation of cyberserfs (i.e. Internet users) by their feudal lords (i.e. modern service providers). Indeed, my original article probably lacked sufficient imagination (or perhaps I lacked the fortitude) to fully describe what might happen.

A. The Extent of the Cybermanor

For example, I underestimated the size of the Internet's cybermanors. When I wrote the article, I envisioned that "estates" would be things like individual services or websites, and that cyberlords would track only what cyberserfs did in cyberspace. I did not envision that the tracking of users would extend deeply into a person's every day, "real life" existence.

---

[12] *See id.* at 1250–53.
[13] *See id.* at 1248–49, 1262–63.

Thus, to my original sensibilities, America Online (remember them?) would be a large estate. Today's largest cyberlords would dwarf AOL. The website Investopedia reported that, as of May 30, 2019, three of the world's largest companies by market capitalization are cyberlords.[14] Alphabet, the parent company of Google, ranked second with a market value of $822.96 billion.[15] Amazon had a capitalization of $795.18 billion.[16] And Facebook had "only" $557.97 billion.[17] Companies get this large in part because they have enormous numbers of cyberserfs, but it is more than that. These cyberlords are incredibly good at using modern digital technology to know a lot more about their cyberserfs than what they do online.[18]

The advent of the modern smartphone means that service providers go everywhere in real life with users. The location capabilities on these devices allow numerous providers to know (and record) a user's whereabouts on an almost continuous basis unless the user disables location tracking or turns off the relevant service provider's app.[19] The list of such providers is long. The cellular service

---

[14] Elvis Picardo, *10 of the World's Top Companies are American*, INVESTOPEDIA, https://www.investopedia.com/articles/active-trading/111115/why-all-worlds-top-10-companies-are-american.asp [https://perma.cc/MVX7-JNCM] (last updated May 30, 2019).

[15] *Id.*

[16] *Id.*

[17] *See* Picardo, *supra* note 14.

[18] *See* Jon Brodkin, *Google Workers Listen to Your "OK Google" Queries – One of Them Leaked Recordings*, ARSTECH NICA (July 11, 2019, 3:31 PM), https://arstechnica.com/information-technology/2019/07/google-defends-listening-to-ok-google-queries-after-voice-recordings-leak [https://perma.cc/99M2-7SQA] (discussing Google Assistant listening to, and Google staff hearing, unintended recordings).

[19] *See* Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret,* N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/4QQA-4VNY].

provider knows where its customer is, and so do travel providers, navigational services, social media companies, retail enterprises, and entertainment providers.[20]

The modern user also wears Internet-connected devices, typically smart watches, that provide even more data to service providers. Heart rate, form of exercise, precise routes taken while walking, and even the number of steps taken all get measured and stored. Smart watches can record sleep patterns and are therefore capable of telling service providers when people awaken and go to sleep.[21]

Similarly, many people have devices in their homes capable of observing some aspect of their lives and "phoning home" with the information. Alexa, Google Assistant, and Siri are "always on" and listening.[22] Even though they are not supposed to record unless activated, reports of "accidental" recordings stored by service providers have raised questions about the things service

---

[20] The apps on my cellphone (an iPhone 6) requesting access to location data include: Apple Maps, the 2019 U.S. Open (tennis), local weather and news apps, airline apps (including Alaska, United, Delta, and American Airlines), ESPN, Ballpark (the app for Major League Baseball), Google, Google Maps, Skype, Waze, and Yelp. *See id.* (stating that thousands of popular apps contain location sharing code).

[21] *See* Matt Hamblen, *As Smartwatches Gain Traction, Personal Data Privacy Worries Mount,* COMPUTERWORLD (May 22, 2015), https://www.computerworld.com/article/2925311/as-smartwatches-gain-traction-personal-data-privacy-worries-mount.html [https://perma.cc/6HHE-KKR2]; Brian X. Chen & Steve Lohr, *With Apple Pay and Smartwatch, a Privacy Challenge*, N.Y. TIMES (Sept. 20, 2014), https://www.nytimes.com/2014/09/11/technology/with-new-apple-products-a-privacy-challenge.html [https://perma.cc/P5Y8-FUQ7].

[22] *See* Jean Baptiste Su, *Why Amazon Alexa Is Always Listening To Your Conversations: Analysis*, FORBES (May 16, 2019, 2:43 AM), https://www.forbes.com/sites/jeanbaptiste/2019/05/16/why-amazon-alexa-is-always-listening-to-your-conversations-analysis [https://perma.cc/3USE-R6AT].

providers learn.[23] Smart devices like refrigerators, coffee makers, and home security offer further ways a service provider might gain knowledge about its users' lives.[24]

Individually, each of these sources of information would comprise a nice cybermanor of its own. But of course, cyberlords share information, making the estates even larger. Furthermore, the use of big data and modern analytics allows cyberlords to make any number of inferences about their users. In some cases, they may even be able to take apparently unrelated anonymized information and determine the real identities of those whose data has been obtained. The consequence of all this is that a few very large cyberlords know a lot about huge segments of a cyberserf's everyday existence, not merely what she does online. It is now possible for a cyberlord to learn when a cyberserf awakens, when and where she goes to work, whether he stops at a gym on the way home to exercise, what he likes to read, the items he buys, and more.[25]

---

[23] *See* Kari Paul, *Google Workers Can Listen to What People Say to Its AI Home Devices*, THE GUARDIAN (July 11, 2019), https://www.theguardian.com/technology/2019/jul/11/google-home-assistant-listen-recordings-users-privacy [https://perma.cc/T57Q-UT2D]; Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time [https://perma.cc/3YBM-QVZ9] (describing how Alexa and Siri are always listening and recording).

[24] *See* Fowler, *supra* note 23 (discussing use of smart devices in home to collect and record personal data).

[25] Facebook's Project Atlas provides perhaps the most egregious example of this. In it, Facebook paid people, including teens, to install an app on their phones that allowed Facebook access to everything on the phone. *See* John Constine, *Facebook Pays Teens to Install VPN that Spies on Them*, TECHCRUNCH (Jan. 29, 2019), https://techcrunch.com/2019/01/29/facebook-project-atlas [https://perma.cc/7E52-HETM].

B. The Extent of Political Power

I also underestimated the political power that would accrue to cyberlords. When I wrote the article, I thought that the extent of such power would be confined to the experience a user had on an individual website. Thus, on an early social media platform like AOL, the cyberlord would literally structure the possibility and terms of communication among its users by monitoring content, choosing to enable mass communication, and selecting the people allowed onto the platform in the first place.[26]

What I did not predict was the extent to which people would make cyberlords their primary intermediaries for obtaining news and political commentary in the real world. Nor did I foresee how profitable it would be for cyberlord intermediaries to, at least in some cases, provide news and commentary with little regard for whether the source of that content was anchored in factual reality or responsible social opinion.

The problem is now well-known. A service provider makes more money (generally from advertisers) when its users remain connected to its service. Users are more likely to keep using a service if they are shown things they like to read. Service providers therefore deploy algorithms to build profiles of their users and offer them content matching the profiles. Because the service provider cares primarily about whether the user will want to read the suggested content, not whether the content is true or responsibly sourced, it is likely that some users will be offered false conspiracy theories or deliberate propaganda masquerading as news.[27] Recent problems at Facebook,

---

[26] *See* Yen, *supra* note 1, at 1240–42.

[27] *See* Center for Information Technology and Society at UC Santa Barbara, *How is Fake News Spread? Bots, People Like You, Trolls, and*

including its role in facilitating the work of Cambridge Analytica and foreign propagandists, exemplify the problem.[28]

The problem of political power even exists when a service provider tries to be responsible. A search engine like Google still effectively controls what its users read. If a political scandal erupts and threatens the electoral viability of a candidate, how many stories about the scandal should the search engine display, and which ones?

The quandary becomes even more apparent when one considers that large cyberlords directly assist political campaigns with advertisements and strategies to maximize influence over the Internet. A 2018 Campaign for Accountability report describes how Facebook and Google embed consultants with major political campaigns to assist with Internet strategy.[29] As the report points out, such political consulting—done free of charge—is of great value

---

Microtargeting, https://www.cits.ucsb.edu/fake-news/spread [https://perma.cc/DL5H-KDG3]; Caitlin Dewey, *What You Don't Know About Internet Algorithms Is Hurting You. (And You Probably Don't Know Very Much!)*, WASH. POST (Mar. 23, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/03/23/what-you-dont-know-about-internet-algorithms-is-hurting-you-and-you-probably-dont-know-very-much [https://perma.cc/T2A8-6GAT].

[28] *See* Matthew Rosenberg & Sheera Frenkel*, Facebook's Role in Data Misuse Sets Off Storms on Two Continents,* N.Y. TIMES (Mar. 18, 2018), https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html [https://perma.cc/2YUC-25PN]; Christian Sandvig, *Corrupt Personalization*, (June 26, 2014), https://socialmediacollective.org/2014/06/26/corrupt-personalization [https://perma.cc/3Q35-ELTV].

[29] *See Partisan Programming: How Facebook and Google's Campaign Embeds Benefit Their Bottom Lines*, CAMPAIGN FOR ACCOUNTABILITY (2018), https://campaignforaccountability.org/work/partisan-programming-how-facebook-and-googles-campaign-embeds-benefit-their-bottom-lines [https://perma.cc/JCH6-DBD6].

to candidates because these companies own the platforms through which the politicians hope to influence voters.[30] Presumably, no one understands how better to game the Facebook or Google news and search algorithms better than Facebook or Google themselves. If the free consulting proves effective, successful political candidates will of course be grateful to those who helped them gain power.[31]

Let us take a moment to reflect on how thoroughly this practice reflects the combination of private property and the political power characteristic of feudalism.[32] A large cyberlord like Facebook or Google owns a huge cybermanor populated by cyberserfs who read the articles and see the advertisements displayed to them by the cyberlord. The cyberlord literally sells the time and attention of the cyberserfs to candidates for political office, knowing full well that its assistance to the political campaign will affect what voters think and for whom they will vote. In fact, Facebook has concluded that it can even influence whether one of its users votes.[33] The cyberlord's

---

[30] *Id.*

[31] *See* Sarah Emerson, *How Facebook and Google Win by Embedding in Political Campaigns,* VICE (Aug. 15, 2018, 9:00 AM), https://www.vice.com/en_us/article/ne5k8z/how-facebook-and-google-win-by-embedding-in-political-campaigns [https://perma.cc/3ABX-ZYMW]; Ryan Mac & Charlie Warzel, *Congratulations, Mr. President: Zuckerberg Secretly Called Trump After the Election,* BUZZFEED NEWS (July 19, 2018, 3:51 PM), https://www.buzzfeednews.com/article/ryanmac/congratulations-zuckerberg-call-trump-election-2016 [https://perma.cc/RN2U-GKRC] (reporting call from Mark Zuckerberg to Donald Trump congratulating the candidate on his successful use of Facebook and its consulting services).

[32] *See* Yen, *supra* note 1, at 1232–36 (describing characteristics of feudalism).

[33] *See* Zoe Corbyn, *Facebook Experiment Boosts US Voter Turnout*, NATURE (Sept. 12, 2012), https://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401 [https://perma.cc/3P4V-MH7U].

consultants give advice to the politician about how to exploit the cyberlord's property (namely the platform and the attention of its cyberserfs) by purchasing ads that surely profit the cyberlord. If the politician wins the election, her gratitude for that assistance will multiply, perhaps in the form of political access that can be used to influence regulation that would otherwise harm the interests of the cyberlord. A cynic could easily argue that such arrangements risk converting a user who thinks he is being given disinterested reading suggestions into a manipulated voter whose vote has been converted into an asset used to help elect a politician that the voter might not otherwise support in the absence of the service provider's active assistance.

Surely Facebook and Google would protest that no conflict of interest exists and that they do not manipulate elections for profit. They would probably claim that the companies provide the same level of service to candidates on both sides of elections. While this may lessen the likelihood of nakedly partisan behavior by cyberlords, it does not change the fact that a given user may be reading something because his supposedly politically neutral service provider has suggested it as part of a political advertising campaign constructed by the provider for profit. Nor does it change the possibility that the service provider could, if it wished, provide this service only to certain candidates.

My purpose here is simply to illustrate that large service providers have acquired great political power, not criticize them for having it. Such power often comes with the accumulation of significant assets, and what matters is that it be exercised responsibly. Indeed, I understand why Facebook or Google might decide to help only certain candidates, at least in some situations. To take an extreme

example, would we think it inappropriate if one of these companies chose not to offer political consulting to a candidate actively espousing eugenics or racial segregation?

It is, of course, a perhaps unsolvable problem to curb the political power that cyberlords have. A clean solution is unlikely to exist, especially in a country committed to the First Amendment. Cyberlords remain private actors entitled to exercise their speech rights largely as they see fit. Even if society chose to treat companies like Google and Facebook as public platforms subject to unusual levels of regulation, I am not sure that this would solve the problem. Indeed, it might even exacerbate the problem.

C. Who or What is the True Emerging Cyberlord?

Finally, I think I may have identified the wrong cyberlord. In the article, I considered government regulation a necessary balance to the excesses of overzealous private actors. Now, however, it is entirely possible that the ultimate cyberlord is government itself.

Each of the methods used by private cyberlords can be used by government to surveil the general population. For example, law enforcement now uses warrants to get information from Google to reveal the identities of those in locations near where unsolved crimes have occurred.[34] This information comes from a database that includes cellular telephone location records going back nearly ten

[34] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police,* N.Y. TIMES (Apr. 23, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/MM6U-J6PW].

years,[35] and it can be very helpful in suggesting persons of interest for further investigation. However, use of this investigative tool means disclosing the whereabouts and activity of innocent people, people whose behavior would not ordinarily be known to the government.

Facial recognition technology might be leveraged even more powerfully. For example, a social media company like Facebook employs facial recognition technology as part of its tagging process.[36] Social media companies will therefore have significant databases that enable identification of individuals from their faces alone.[37] These databases could, in theory, be combined with libraries of images compiled by government, whether through driver's license photos or images taken at airports, border crossings, buildings, and other public locations to amplify other information to create records of where people have been, whether or not they have done anything to warrant surveillance.

That government has not yet taken such steps, or that such efforts are presently limited, offers little comfort. The disclosures of Edward Snowden suggest that the United States is fully capable of spying on its own citizens.[38] It does not take a hugely fevered imagination to

---

[35] *Id.*

[36] *See* Camila Domonoske, *Facebook Expands Use of Facial Recognition to ID Users in Photos,* NPR (Dec. 19, 2017, 1:39 PM), https://www.npr.org/sections/thetwoway/2017/12/19/571954455/facebook-expands-use-of-facial-recognition-to-id-users-in-photos [https://perma.cc/CM8U-9JH8].

[37] *See* Cade Metz, *Facial Recognition Tech Is Growing Thanks to Your Face*, N.Y. TIMES (July 14, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html [https://perma.cc/6C4E-48XX].

[38] *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret*

posit a future in which government works closely with cyberlords to share information that maintains mutual commercial and political advantage. Private enterprise cyberlords provide information and political assistance to government, which in turn maintains a favorable regulatory and economic environment for cyberlords. Obviously, I am not making the direct claim that something this extreme has already happened. I am, however, pointing out how technology makes it possible.

III. CONCLUSION

Looking back, I can confess that the article under discussion here has been a bit of a puzzle to me. I consider it a fairly interesting use of metaphor to create insights that time has proven correct. The Internet has as much potential to oppress us as it does to liberate us. Yet, as a piece of scholarship, I am not convinced it was particularly successful.

When compared to other scholarship I have written, the article is cited less frequently. And, when I tried to place the article, I had some difficulty because law review editors did not know what to make of it. I spoke to one editor who told me that the piece was perhaps the most interesting that he had read, but he didn't know what the journal would do with it. I'm not without sympathy for his point of view. After all, the article has almost no traditional case analysis, nor does it offer some large

---

Program, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/BFR3-9MYH]; Ewan Macaskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [https://perma.cc/V5GA-D7 AU].

theoretical framework. I did not then, nor do I have now, a really good solution to the problem of oppression through the Internet. These are shortcomings.

Perhaps the article would have been more successful if I had been more imaginative or daring. Maybe I could have foreseen the things discussed above, making my ideas more provocative. Yet, I'm also not enough of a futurist to have seen all of this coming, and legal scholarship is not a genre where speculation is encouraged. In the end, though, I suppose I can be satisfied that I can stand by what I wrote seventeen years ago, and I am grateful for a chance to revisit the work and update its message.