In tracing the history of social media, one might begin with late eighteenth-century English coffeehouses: full of passionate debates, open to all comers, and cited by some as the downfall of education and workplace productivity. In fact, Tom Standage (2013) draws this analogy in an upbeat *New York Times* piece on the state of digital technologies. “There is always an adjustment period when new technologies appear,” Standage reassures us, and while disruptions may occur, “the lesson of the coffeehouse is that modern fears about the dangers of social networking are overdone.”

Such glossing histories are ripe for criticism: those coffeehouses were bastions of masculine privilege. Technological differences trouble simple comparisons. Indeed, to rest assured of the beneficence of new social spaces is to abandon responsibility for their legal and cultural development. This is especially true during critical junctures in which policy decisions—often made behind closed doors—set the course of development for decades. An “adjustment period” is precisely the time to err on the side of prudent foresight, as technical protocols tend to become locked in, hardware and software become path dependent, and network effects tend toward monopoly and economic disenfranchisement (Lanier, 2013; McChesney, 2013). As Grossweiler (2012) suggests,

> If you expect that a new medium is neutral and simply additive, the unexpected consequences will be negative. If you expect that a new medium will have only a positive impact, the consequences also will be negative. But if you anticipate that a new medium will have negative consequences, the consequences are more likely to be positive.  

(pp. 92–93)

While determinism of any stripe is to be avoided, current discourses tend toward self-serving celebration. But blind faith in the inherent beneficence of new technologies cedes ground to those power players who have come to shape the field. The idealistic dreams of early internet researchers and counterculture hackers, of advertising-free collaboration and free exchange, have given way to a commercialized landscape in which users are treated as audiences to be sold to the highest bidder. To recapture Standage’s analogy, a handful of elites not only own the coffeehouses, but efficiently track customers in their movements, conversations, and preferences—allowing them to nudge conversations and consumer choices in directions favorable to the bottom line.
WHO DEFINES “SOCIAL MEDIA”?

The dominance of commercial forces in shaping social media is exemplified by the fact that marketers have authored most of the articles aimed at defining the term. Essentially, social media overturns the one-way model of radio and television broadcasting by involving audiences in content production. Early Web 1.0 predecessors of today’s popular social media platforms include chat rooms, listervs, and instant messaging services like AIM and ICQ. Relationship-based sites like Classmates.com were popular in the mid-1990s, and the turn of the century spawned various community sites with limited “friends” functionality, like AsianAvenue, MiGente, and BlackPlanet (boyd and Ellison, 2007, p. 213). Launched in 1997, SixDegrees.com was the “first recognizable social network site,” paving the way for Web 2.0 sites like MySpace and Friendster—which in turn were displaced by Facebook, Twitter, Google+, Second Life, and LinkedIn (p. 214).

Though immensely popular, such social networking sites are a sub-set of the broader category of social media, which includes a variety of platforms and applications that enable interactivity and sharing. Many platforms encourage user-produced content, including YouTube for video, SoundCloud for audio, and Instagram, Flickr, and Pinterest for photographs. Users often share content from such platforms on social networking sites, and in some cases (like YouTube and Google+), content-sharing and social networking platforms are owned by one company. Music streaming sites like Pandora and Spotify allow sharing of user-created stations. Sites like Digg and Reddit enable news sharing, as do plug-ins like StumbleUpon, which run on social networking platforms or browser software. Wikis and blogging platforms like WordPress allow visitors to post comments and engage in discussion. Protocols that enable sharing and accessing of blogs like RSS (Really Simple Syndication) also fall under this broad category. Any platform, application, or widget that enables participation, collaboration, sharing, community formation, or augmentation of real-time events may be considered social media.

There is a danger, though, in painting emergent media with too broad strokes. Lumping together different platforms and projects under the generic headings of social media, Web 2.0, or “the internet” obscures their ethical and political differences (Morozov, 2013). As Catherine Coleman (2013) argues,

> When used in celebratory terms, Web 2.0 puts on equal footing a user who uploads a video on YouTube or a photo on Flickr (corporate-owned, proprietary platforms) and a free software developer or even a Wikipedian who is part of a nonprofit, collective effort. (p. 208)

Technologies simultaneously reflect and shape culture, so it is important to understand differences in the values that drive emergent projects. Social media platforms do not always resemble coffeehouses, and those that do may serve not as bridge-building seminars but bastions of hate speech. The struggle to define social media in both technical and moral terms is ongoing.

APPROACHING ETHICS IN SOCIAL MEDIA

An ethics of social media cannot afford to indulge naïve assumptions of technological neutrality or sweeping claims of technological determinism (positive or negative). Values and norms drive development, and digital technologies can encode ideas about how information should be managed, stored, and exchanged. Yet human judgment remains indispensable. While technologies
may exhibit limited functional neutrality (a gun can be used to protect or to murder the innocent), such neutrality presupposes a moral ecology fundamentally transformed by the affordances of such technologies (a world with guns is a different moral landscape than one without). Despite the intentions of developers, technologies alter moral ecologies in unpredictable ways. As new technologies create systemic disturbances along certain value axes, they generate impassioned debate and renegotiations of social norms. For example, early internet subcultures (counterculture movements, hackers, researchers) valued collaboration and openness, developing protocols and infrastructures intended to support such values. Yet commercial and government interests have exploited these infrastructures to enhance consumer and military surveillance operations. Users and participants who make due within these confines face exploitation, privacy violations, and dehumanization (Solove, 2004, p. 47). Technologies do not operate deterministically either in positive or negative ways, but through their unique affordances force the attention of human judgment toward certain axes of value. Technological development therefore does not overcome, but instead both involves and necessitates, ongoing political struggle.

Unfortunately, popular debates are driven by myopic assumptions about technology that obscure rich understandings of the long-term implications of social media. Discourses of social media ethics are driven largely by corporate and military interests, which have a vested interest in framing technology as politically and economically democratizing. Ideologies of online ethics are produced and managed in ways that benefit commercial and governmental interests at the expense of the public. Meanwhile, users and consumers tend to focus on social privacy (which of my friends can see my status update?) while neglecting complex issues of informational privacy (what third party organizations have access to my personal data?). Commercial news coverage exacerbates these issues by, for example, highlighting the personal saga of whistle blower Edward Snowden while failing to address the systemic issues that his leaked information uncovers.

The key players in public debates (corporations, governments, consumers, activists) each approach social media ethics from a perspective limited by some combination of ignorance, shortsighted self-interest, and techno-centric ideology. Due to their unique affordances, social media disrupt moral ecologies along the fault lines of specific axial values including autonomy, authenticity, responsibility, and trust (Bugeja, 2009; Healey, 2010). As a result they provoke debates about social norms like privacy and consent. Corporate and government rhetoric about the benefits of transparency redefines privacy norms at the expense of consumer, user, and activist rights. The death of privacy is sold as a route to authentic self-expression, but transparency in the digital economy typically functions as a one-way mirror, eschewing reciprocity in favor of perpetual surveillance operations that bolster vested power structures. Corporate privacy policies and legislative frameworks that expand military surveillance undermine substantive notions of consent in favor of control and coercion. Rhetoric about the democratizing benefits of interactivity obscures issues of labor exploitation and the externalization of risk (Lanier, 2013, pp. 59–63). Celebrations of the benefits of big data, whether for consumers or national security, obscure issues of reputation control and individual autonomy. In other words, the “media regimes” that characterize the digital era are accompanied by ideological or normative regimes that tend to undermine the achievement of human dignity (Williams and Delli Carpini, 2009). To realize the democratic potential of social media requires a recognition and rejection of the common assumptions that drive popular debates.

Consumer Surveillance and the Coercion of Consent

An individual’s ability to control the relative openness of one’s personal boundaries is central to the achievement of autonomy and authenticity (Margulis, 2011, p. 12; Trepte and Reinecke, 2011, p. 62). Yet even before the arrival of social media, executives proclaimed the irrelevance
of online privacy. In 1999, Sun Microsystems’ CEO Scott McNealy stated flatly, “You have zero privacy anyway. … Get over it” (Sprenger, 1999).

Such extraordinary statements, which redefine basic privacy norms, reflect the commercial interests driving most social media platforms. In its early years the internet was largely a non-commercial and even anti-commercial institution (McChesney, 2013, p. 97). In the mid-1990s, however, the backbone of the internet was turned over to the private sector (p. 104). While companies like Google initially rejected the idea of relying on advertising, today they depend on it for their livelihood (p. 102). Commercial social media platforms treat users as a means to an end, cultivating vast databases of user information to be sold to advertisers.

Not surprisingly, such companies downplay privacy issues and instead proclaim the benefits of data collection—namely that advertisements and social news feeds will be more personalized and relevant. In general, users are unconcerned about how their data is used by third parties, as long as they can manage how it is shared with friends. In other words, they tend to focus on social privacy rather than informational privacy, protesting loudest when the former is compromised. Facebook faced a massive backlash in 2007 for its Beacon program, which announced users’ consumer purchases from partner websites in Facebook’s news feeds. A U.S.-based class action lawsuit, premised on the notion that any such announcement requires user consent, ended the program. Watchdog groups in Canada and Norway raised similar complaints. In 2009, Facebook nevertheless changed its privacy settings so that users’ actions defaulted to “public.” In explanation, Mark Zuckerberg said that people had become more comfortable with openness and sharing, and Facebook had simply “decided that these would be the social norms now” (Frum, 2012). Numerous reports summarized Zuckerberg’s statement under the headline “privacy is dead.”

While users—especially teens—are concerned about social privacy, they tend to be unaware of informational privacy issues. Parents express some concern about how much information advertisers can collect about their children, but teens have little understanding or concern about third-party data use (Madden et al., 2013). As a result, many forego reasonable steps to protect informational privacy (Facebook and your privacy, 2012). However, breaches of informational privacy have long-lasting impacts. Third-party companies have used such data to deny individuals insurance coverage, lower their credit scores, and target them with discriminatory pricing schemes or ads that reinforce gender and racial stereotypes (Andrews, 2013, pp. 35–37).

Companies like Facebook and Google approach issues of consent in ways that reflect distinctly U.S.-based models of privacy. European models are more deontological, viewing privacy as an inalienable right even if its protection has negative economic impacts (Bodle, 2011, p. 159). In the E.U. data are protected by default and users must opt-in, while in the U.S. data is collected by default and users must opt-out (p. 160). The U.S. takes a utilitarian or “interest-based” approach through industry self-regulation, on the principle that business access to user data provides “the greatest good for the greatest number” (pp. 159–160). This approach focuses on professional codes of conduct, user contracts, and norms within the industry, placing the burden on users to trust in these companies’ good faith.

Google, for example, actively cultivates a sense of trust among its users as part of its public relations and branding efforts (pp. 160–161). If users trust the company with their data, they are more likely to click through user-end agreements, even if such agreements are so complex as to render informed consent meaningless (Nissenbaum, 2011). Vague language in such agreements obscures how often collection and sharing occurs. Justifications for data collection focus on user rather than company benefits, constructing a binary choice between privacy and quality of service (Bodle, 2011, pp. 161–163). Furthermore, while companies insist that users have the choice to opt-out, they actively “nudge” user decisions through the effective use of “choice architecture”
In summary, their approach to securing consent is one of soft coercion, including reassurances of the benefits of disclosure, obfuscation through self-serving legal terminology, subtle choice architecture, and legal strong-arming.

**Technologies of Intimacy and Revenge**

Ironically, the same corporate entities declaring openness as the new social norm benefit from tight intellectual property and technical barriers that keep algorithms and databases sealed from public and competitor scrutiny. Media and legal discourses place primary importance on the protection of profit-generating information, while framing private sexual content as uncontrollable and therefore beyond the reach of legal protection (Hasinoff, 2015, p. 134). In fact, the assumption is that social media users consent to the distribution of private data by the mere act of participation. Transparency is a one-way street: privacy is dead for thee, but not for me, declare the social media giants.

Beyond buttressing corporate power, such libertarian models of information have the broader cultural impact of solidifying entrenched cultural ideologies of sexuality and gender. As Hasinoff (2015, p. 137) argues, “private sexual images can be seen as a non-normative sexual behavior and thus not deserving of privacy.” In this light, consider Google CEO Eric Schmidt’s well-reported statement on privacy: “If you have something that you don’t want anyone to know,” Schmidt remarked in 2009, “maybe you shouldn’t be doing it in the first place” (Streitfeld, 2013). A year later, Rutgers University student Tyler Clementi committed suicide after his roommate, Dharun Ravi, surreptitiously used a webcam to view Clementi’s romantic encounter with another man. Via Twitter, Ravi invited friends to view a second encounter either in his room or via iChat. Clementi jumped to his death from the George Washington Bridge before Ravi could hold his viewing party. The tragedy underscores the fact that, as Natasha Lennard (2013) explains, corporate notions of transparency are “underpinned by an immense privilege” since those who boast of having nothing to hide rarely identify as racial, political, or sexual minorities.

Numerous court battles and public debates about sexting—the sending and receiving of sexually explicit texts, photos, or other messages—demonstrate how libertarian information policies buttress traditional hetero-normative standards of gender and sexuality. Hasinoff (2015) argues that school and law enforcement authorities fail to make meaningful distinctions between consensual sexting, where the participants’ goal is pleasure and communication, and abusive sexting, where a perpetrator—usually male—distributes a partner’s image without her consent. This framework “has damaging effects, particularly for girls, who are more likely to be both humiliated and punished if their sexual images circulate widely” (p. 133). In one case, two cheerleaders were suspended from school for sexting, while the boys who shared their private images were left unpunished (p. 140). In the court system, legal models are problematic because they view any production of explicit underage material as child pornography. In 2009, for example, a fourteen-year-old girl was arrested for posting nude pictures of herself on MySpace (Lunceford, 2011, p. 103). Thus it is possible that, upon reporting an incident of abusive sexting, the victim may be prosecuted for the production of child pornography.

Such cases suggest that even as young people are developing their own norms to protect privacy in the context of consensual sexting, legal systems lack the nuance required to address the complexity of adolescent sexuality in the digital environment (Lunceford, 2011, p. 103). Hasinoff (2015, p. 139) argues for the adoption of an “explicit consent” model that would introduce technical and legal restrictions on the non-consensual production or distribution of private content by individuals, businesses, or governments. This approach might address the gender imbalance
that tends toward leniency for young men who maliciously distribute images while criminalizing young women who may have initially produced the images in a consensual context.

As in the case of consumer data collection, however, the line between consent and coercion is unclear. Cultural pressures toward the sexualization of young women, coupled with commercial incentives to develop applications that afford more frequent and intimate communications, suggest that even consensual sexting may be considered a form of self-exploitation (Lunceford, 2011, p. 106). Lunceford rejects such a stark assessment, arguing from a utilitarian perspective that sexting teens are seeking happiness as they understand it. Even so, he notes that this search unfolds in a context in which young women encounter sexualized images of other teens, such as Miley Cyrus’s suggestive photo spread in *Vanity Fair*—images that, if produced by private individuals, might be considered child pornography (p. 102). In this sense, “adolescents who engage in sexting seem to have internalized the sexualization of the world in which they live” (p. 109). Applications developed to enhance user control over explicit images, such as Snapchat, arguably contribute to such cultural pressures by streamlining the technological affordances that enable such communications. Citing Ellul, Lunceford argues that “teens who engage in sexting are pushing the boundaries of adolescent sexuality in ways that have less to do with the adolescents themselves and more to do with the technologies available to them for expression of those desires” (p. 112).

Traditional social media platforms stand to gain, if inadvertently, from the proliferation of such applications. While applications like Snapchat tout themselves as privacy enhanced, groups like the Electronic Privacy Information Center claim that they misrepresent their data security practices (Guynn, 2013). Time-limited photos can be screen-captured, and past photos are retrievable with proper technical know-how. Thus Facebook and Tumblr groups have formed where users post captured Snapchat nudes. Yet the privacy policies to which these companies coerce users’ consent are written not to protect users from such exploitation but to protect the implicated companies from liability when abuses occur.

While mainstream companies benefit indirectly from the exploitive use of sexting applications, rogue entrepreneurs like Hunter Moore and Craig Brittain have developed platforms whose revenue models are premised on the non-consensual distribution of explicit images. “Revenge porn” websites generate traffic and ad revenue by allowing users to upload explicit images of people—usually a male user’s ex-girlfriend—without their consent. In some cases these images are linked directly to the Facebook or Twitter profile of the victim. In defense of his business model one revenge porn developer, Craig Brittain, invoked rhetoric that echoes Mark Zuckerberg’s idealistic view of transparency. “It’s part of a progressive cause,” Brittain told host Bob Garfield of *On the Media*, explaining that “my eventual goal is that everyone will have public information posted about them, preferably naked, that it’ll be a normal thing. It’ll no longer be associated with stigma or shame or humiliation, but it will be normal” (“Is Anybody Down?”, 2012). Presumably such new norms of disclosure would usher in an era of unbounded, authentic self-expression. In the meantime, however, Brittain operated the site as an extortion scheme, placing ads for a phony law firm next to the photos and enticing victims to pay a fee to have them removed.

While private corporations have established a robust legal apparatus to protect copyrighted material and other intellectual property, the legal system has been slow to address issues of abusive sexting. Following the Tyler Clementi case, New Jersey became the first state to pass legislation addressing revenge porn, followed by similar proposed bills in Florida and California. By early 2019, over 40 U.S. state legislatures had addressed the problem directly. New York was among the last to follow this trend, passing its version of a revenge porn law in March of 2019 after a long period of opposition from tech companies. For their part, advertisers (including third-party providers like Google) have begun to respond to boycotts of social media sites
like Ask.fm, which was implicated in the cyber-bullying and subsequent suicide of 14-year-old Hannah Smith (Topping and Coyne, 2013). Yet it is clear that social media companies largely steer the ship when it comes to legislation addressing privacy and consent, in ways that consolidate corporate power while externalizing risks to individual users, with social minorities bearing the brunt of the burden.

**Government Surveillance and Corporate Collusion**

State regulatory agencies are ostensibly positioned to protect the public against privacy abuses. Yet in the U.S. especially, legislators and executives share a common reverence for networked technologies as a sacred source of economic productivity and democratic freedom. Policies are crafted on the premise that digital networks are an extension of natural ecological systems, from which perspective any regulatory interference is a violation of natural law, if not God himself (Healey, 2013). Not surprisingly, oversight is meek. In response to complaints of deception with regard to user privacy, in 2011 the U.S. Federal Trade Commission reached a settlement with Facebook and Google that subjected each company to twenty years of privacy audits. The companies would be able to hire their own auditors, however, and would be able to keep the resulting reports from the public in the interest of protecting trade secrets (Hill, 2011).

These companies’ subsequent behavior has not been reassuring. Two years after the FTC settlement, German regulators fined Google 145,000 Euros for illegally storing e-mails, passwords, and images collected from home wireless networks by its Street View cars—a fine amounting to a mere 0.005 percent of the company’s annual profits (Ferenstein, 2013). Meanwhile, the FTC determined that Facebook may have violated its 2011 agreement by enabling the massive privacy scandal surrounding the Cambridge Analytica data firm. As of this writing, Facebook and the FTC are negotiating what may be the largest-ever fine against any tech company.

Governments’ role in protecting the public is not only legally and financially meager; it is fundamentally compromised by military and national security interests. As McChesney (2013) notes, the relationship between social media companies and the national security apparatus is not adversarial but “complementary and collegial, even intimate” (p. 162). Cheaper and more reliable than government employees, one critic describes the internet as “a surveillance tool made in heaven” (p. 161). Social media websites are invaluable in this regard. The U.S. Department of Homeland Security searches sites like Facebook and Twitter to assess public reaction to proposals under consideration (p. 165). The Internal Revenue Service searches social media for evidence of tax evasion, and the U.S. Citizenship and Immigration Services relies on these sites to search for immigration fraud. The National Security Agency is developing its own storage facilities for user data, much of which is collected from social media platforms like Facebook, YouTube, and Skype through the once-secret PRISM program. In fact, one reporter described PRISM as “a social media version of a Bush administration program” that had been designed to track terrorist financing (Wertheimer and Temple-Raston, 2013). Echoing corporate rhetoric that frames user-end policies as a binary choice between consumer benefits and personal privacy, government rhetoric frames such top-secret surveillance programs as a stark choice between national security and Fourth Amendment rights.

Social media companies stand to benefit from cooperation with government surveillance initiatives. Network effects tend to generate monopolies in internet service providers (ISPs), search engines, and social networks. This process makes government data collection easier and therefore provides little incentive to break up concentrated markets. AT&T and Verizon—a virtual duopoly in wireless service—employ dozens to respond to law enforcement requests for surveillance data (McChesney, 2013, p. 112). As these companies seek subsidies and tax benefits
from legislators, compliance with government requests is more likely. Legislation like the Cyber Intelligence Sharing and Protection Act (CISPA), which passed the U.S. House of Representatives in 2012, provides both government access to such data and legal protection to companies who share it (p. 167). ISPs are often paid for cooperation with law enforcement efforts, and third-party companies like LexisNexis offer products designed to provide social media data to law enforcement (p. 165). Some U.S.-based security technologies are sold to authoritarian governments in China and Pakistan, troubling the self-serving refrain that digital technologies are an inherently democratizing force (p. 163). In fact, the U.S. military has made copyright and patent protection “an integral part of cyberwarfare,” so much so that the U.S. federal government often acts “like a private police force for the internet giants” (p. 162).

Social media companies responded to the disclosure of the top-secret PRISM program with indignant denials, and Google pressed for measures allowing it to disclose more details about the government data requests it receives. But Google’s rhetoric about transparency is premised on the assumption that any resistance to disclosure—whether from citizens or government—is an admission of guilt. It is a radically conservative notion of transparency since, as Lennard (2013) explains, “that which can be transparent, without fear of persecution, will always be co-extensive with that which poses no real threat to the current socio-politico-economic status quo.” In other words, the same ideology of transparency that renders vulnerable a sexual minority like Tyler Clementi will do likewise for dissidents, activists, and other political minorities. While the quieting of political dissent is obviously beneficial to state power, it is advantageous to a social media companies like Google as well, since the latter understands controversial content on YouTube not as the flourishing of dissent but a primary cause of lost advertising revenue (Andrejevic, 2009). As personal data disappears behind the firewalls of laissez-faire policies that protect corporate trade secrets and undisclosed military surveillance programs, a Kafka-esque scenario emerges in which unaccountable bureaucracies treat dehumanized citizens in a spirit of profound indifference (Solove, 2004, p. 55).

ANONYMITY AS COUNTER-ETHOS

As profit-driven social media companies, in conjunction with military interests, seek to establish compulsory sharing and disclosure as new social norms, activists have sought to build alternate social media platforms where privacy and anonymity are valued as foundational elements of political freedom and human dignity. As part of a broader free and open-source software (F/OSS) movement, some of these include the collaborative knowledge platform Wikipedia, the Linux open-source operating system, grassroots collectives like Indymedia, the non-profit social networking platform Diaspora, and the whistle-blowing organization WikiLeaks. Through such means, activists harness digital media to establish deep social ties and buttress political movements (C. Coleman, 2013, pp. 209–210).

The cyber-vigilante movement Anonymous exemplifies this development, having made effective use of social media to mobilize support for the Arab Spring, U.S.-based and international Occupy networks, and WikiLeaks (Coleman, 2012, p. 94). In ways that highlight the biases of digital networks toward information disclosure, Anonymous seeks to reverse the one-way transparency of corporate and military surveillance by turning digital networks into citizen-wielded tools of vigilance that expose corporate and political malfeasance while protecting the privacy of activists—symbolized by its use of the iconic Guy Fawkes mask (p. 87).

As Coleman explains, while the group lacks a “programmatic plan to topple institutions or change unjust laws,” it nevertheless succeeds in making their evasion “seem easy and desirable”
Through its strident critique of the technology industry, furthermore, Anonymous “offers a provocative antithesis to the logic of constant self-publication, the desire to attain recognition or fame”—one which many scholars and activists find “profoundly hopeful” in the context of persistent corporate and military surveillance (p. 92). Through its coordinated actions, the group frames anonymity as a political practice that maintains the crucial distinction between one’s public and private selves, even as powerful institutions seek to collapse that distinction. In doing so, Anonymous suggests that citizens “must be the guardians of their own individuality, or determine for themselves how and when it is reduced into data packets” (p. 94).

Emerging from the online image board 4chan, which began in 2003 and is known as “one of the most offensive quarters of the internet” for its celebration of pornography, Anonymous was characterized early on by an ethos of mischievousness (p. 83). “Trolling” has long been part of this ethos, as exemplified by the group’s dedicated denial of service (DDoS) attacks, prank calls, and other actions against the Church of Scientology. While still embracing “pre-political” prankster-ism, over time the group’s actions have taken a more political tone, including a focus on issues of free speech and corporate or government deception (p. 87). Recently, the group has engaged in public shaming of young men who have raped women, captured their assault with photographs or video, and publicized it through social media (Swash, 2013). In such cases, the group frames its campaigns as attempts to spur unresponsive law enforcement agents and legal systems into action.

Through actions that resulted in numerous arrests in the U.S. and abroad, Anonymous has also aligned itself closely with WikiLeaks, an organization that depends on social media to such an extent that it developed its own encrypted social networking platform called Friends of WikiLeaks. In response to WikiLeaks’ 2010 release of the Afghanistan war logs (a collection of secret documents leaked by U.S. intelligence analyst Bradley Manning), organizations including PayPal, Visa, MasterCard, and Amazon refused to handle financial transactions or internet traffic for WikiLeaks. In response, Anonymous coordinated DDoS attacks against these organizations, causing millions of dollars in financial damages. In 2011, the group launched Operation HBGary against CEO Aaron Barr of the security firm HBGary Federal. Internal documents revealed that Barr, in conjunction with Bank of America, had planned to undermine WikiLeaks by submitting fake documents and subsequently exposing them (Coleman, 2012, p. 91). Hacking into Barr’s accounts, Anonymous released his private e-mails through the Pirate Bay bit torrent website and defaced his Twitter feed while publicizing its actions in separate tweets.

While these campaigns demonstrate that activists can harness digital networks to reverse the trend toward one-way, pro-corporate transparency regimes, they also highlight the need to develop a more robust ethics of social media activism. Reflecting on Operation HBGary, Coleman notes “there is something deeply ironic and troubling about … unveiling a person’s identity, name, phone number, social security number” in order to make a point about the need for privacy and anonymity (p. 92). In fact, some Anonymous members “took issue with the collateral damage wrought by Operation HBGary, especially the excessive leaking of personal information,” and others criticized “the necessarily clandestine nature of such hacks” as running “counter to the ethos of transparency” (p. 91). Critics have raised similar complaints about the group’s actions on behalf of rape victims, suggesting that their efforts to expose the identities and personal details of rapists could easily frame innocent young men as perpetrators. Former Anonymous member Jennifer Emick also accuses the group of hypocrisy, having received highly misogynistic and sexualized threats after breaking from the group (Swash, 2013).

These episodes reveal that, whether voiced by corporate or anti-corporate actors, the motto of “transparency for thee, but not for me” is ethically unsustainable. In fact, the F/OSS movement’s techno-centric ideology mirrors the corporate-military sacralization of digital networks
(Lanier, 2013, p. 316). For such reasons scholars like MacKinnon (2012) remain skeptical of cyber-vigilantism as a counter-hegemonic strategy, insisting instead on the development of institutional and legal models that can strike a balance between privacy and transparency with prudent judgment and accountability (pp. 26–27).

THE DEATH (AND LIFE) OF JOURNALISM

While Anonymous offers no clear program for institutional reform, the emergent models of journalism forged by cooperation between bloggers, activist organizations like WikiLeaks, and traditional news sources like The Guardian have managed to put both corporations and governments on the defensive with regard to mass surveillance of consumers and citizens. As “the nation’s early warning system,” this watchdog role is, in fact, the first task of journalism (McChesney, 2013, pp. 83–84). Yet the trend toward online commercialism threatens to undermine the potential for journalists to harness social media in ways that bolster this watchdog role.

Coverage of the 2013 Boston bombings demonstrates the potential for social media to damage law enforcement efforts, stir up racial and religious hatred, and harm innocents through false accusation. Through platforms like 4chan, Twitter, and Reddit, armchair detectives cast suspicion on at least four innocent people. Siva Vaidhyanathan called the developments “one of the most alarming social media events of our time,” noting that “we’re really good at uploading images and unleashing amateurs, but we’re not good with the social norms that would protect the innocent” (Bensinger and Chang, 2013). In the rush to stay ahead of possible developments, mainstream news coverage suffered from similar lapses in judgment. Police had to ask the Boston Globe to remove address information the Globe had tweeted about SWAT team operations and, in perhaps the most egregious incident, two innocent Moroccan-American men sued the New York Post for the front-page publication of an amateur photograph of the men accompanied by the headline “Bag Men.”

Journalists’ relationship with more sophisticated social media organizations like WikiLeaks is likewise ethically fraught. Papers like The Guardian assume significant responsibility when reviewing and publishing documents such as the Afghanistan war logs, since they may face charges of causing collateral damage (Elliott, 2013). Lovink and Riemens (2013) argue that leak organizations must establish a robust ethical framework in order to ensure protection both of whistleblowers and any individuals mentioned in leaked materials. While supporters praise the release of damning information that exposes malfeasance, such concerns threaten to undermine the potential of social media to bolster journalism’s watchdog role. “If publishing is not carried out in a way that is absolutely secure for all concerned,” they argue, “there is a definite risk that the ‘revolution in journalism’—and politics—unleashed by WikiLeaks will be stopped in its tracks” (Lovink and Riemens, 2013, p. 252). This point was driven home in the aftermath of the 2016 U.S. Presidential campaign, when investigators discovered a pattern of troublesome communications between WikiLeaks’ founder Julian Assange and Trump campaign advisor Roger Stone.

Ward and Wasserman (2010) argue that such concerns call for “an open approach to journalism ethics” that would “regard the code of ethics as intended not just for professionals but also for anyone who uses media to do journalism” (p. 277). Ethical frameworks should include “all users of media insofar as their tweets, blog comments, and social media sites affect others” (p. 281). Such inclusion should not be limited to solicitations for feedback with regard to accuracy, for example, but the meaningful participation of users in decisions about content, editorial judgment, and organizational management.
While Ward and Wasserman cite *The Guardian* as exemplary in its efforts to forge an open ethic (p. 286), commercial pressures have led most news organizations to over-rely on the speculation of amateur social media while avoiding entanglement with more sophisticated, but politically controversial, organizations like WikiLeaks. In the case of U.S. National Security Agency (NSA) whistleblower Edward Snowden, even the most scrupulous efforts to ensure the judicious release of information were met in mainstream media with accusations of wrongdoing against Snowden, WikiLeaks, and *Guardian* reporter Glenn Greenwald. Greenwald (2013) argued that if Snowden had intended harm to the U.S., he could have sold or released the information in toto. Instead he chose to work closely with a legitimate news source, selectively releasing documents to the *Guardian* and allowing the paper to exercise its own editorial judgment. “The public needs to know the kinds of things a government does in its name,” Snowden explained, “or the ‘consent of the governed’ is meaningless” (“Edward Snowden,” 2013). Nevertheless, coverage in the U.S. often focused on Snowden’s personal saga in ways that displaced substantive debate about the released information and adhered closely to U.S. officials’ narrative of national security and espionage—a problem exemplified by *Meet the Press* host David Gregory’s suggestion that Greenwald had “aided and abetted” Snowden (Beaujon, 2013). While the *Washington Post* also reported on documents it received from Snowden, the paper’s subsequent acquisition by Amazon CEO Jeff Bezos caused some concern among critics, as Amazon had cooperated willingly with the U.S. State Department in refusing its hosting services to WikiLeaks.

The issues of corporate and government collusion that impede efforts to bolster consumer privacy thus have equally troubling implications for the watchdog function of professional journalism. Yet cynical cries about the internet’s inherently destructive impact on journalism are just as guilty of misguided technological determinism as celebratory calls to let the Internet “work its magic” in resuscitating the industry (McChesney and Nichols, 2011, p. xvi). Looking beyond the naiveté of celebrants and the cynicism of skeptics, the potential exists to develop social media platforms, ethical codes, and regulatory policies that support basic democratic values and the institutions that protect them.

**BUILDING A VIRTUAL COFFEEHOUSE**

Recapturing the democratic potential of social media requires rejecting the “catechism” of market ideology that has come to drive public debates about consumer privacy, industry regulation, and national security (McChesney, 2013, p. 23). Tech leaders and their critics alike are guilty of perpetuating taken-for-granted myths of the free market. In lofty rhetoric touting Facebook’s internet.org initiative—a multi-telecomm partnership effort to bolster global internet access—Mark Zuckerberg frames connectivity as a human right (Dredge, 2013). Yet Facebook’s plans, and similar ones at Google, neglect the concern that third-world users have about government surveillance, the role of corporate accountability in protecting connectivity rights, and the conspicuous lack of not-for-profit social networking platforms. To spearhead such initiatives reveals not only their aspiration to dominate emerging markets but their acceptance of the myth that a market-based media system is inherently democratic (McChesney, 2013, p. 63). In his otherwise incisive critique of the imbalance wrought by “siren servers” like Facebook, Amazon, and Google, Silicon Valley’s most credible insider-critic, Jaron Lanier (2013), capitulates to the same misconception. Rather than rejecting the commodification of private data, Lanier suggests that we extend it by requiring companies to offer nano-payments to individuals whenever the use of their personal data increases revenue streams. This arrangement, he argues, will create a more level playing field of “first-class economic citizens” (p. 248). But such approaches create
a “property interest” in information that tends to undermine collective, rights-based protections for user data (Bodle, 2011, p. 160). Tellingly, Lanier limits his discussion to market-based issues like equitable compensation for user-generated content, leaving issues like military and government surveillance off the table.

As Morozov (2011) argues, popular misconceptions about the nature of technology must likewise be rejected. Whether pro- or anti-corporate, current arguments are driven by myopic ideologies that mistake network-enabled transparency and anonymity as ends in themselves—usually deployed in a partisan and self-serving fashion. Neither the total transparency of public communication to governments (e.g. the Total Information Awareness program in the U.S.) nor the total transparency of corporate and governmental behavior to the public (arguably the goal of some activists) is sustainable, however. Techno-centric ideologies reject prudence in favor of unbridled development, either with the deterministic assumption that its direction and impacts are predictable and beneficial, or the simplistic notion that potential harms can be minimized through consumer choice. Rather than ends, transparency and anonymity are a means toward enhancing the values of freedom, accountability, and trust (Craft and Heim, 2009, p. 219). Judgment is therefore paramount, and the institutions of government and journalism have more—not less—of a role to play in the digital economy.

A commons-based approach, by contrast, argues that a democratic media system must include significant elements that are independent from both the state and corporate institutions (McChesney, 2013, p. 66). Such a framework approaches mass media in terms of public goods—that is, “something society needs, but the market cannot produce it in sufficient quantity or quality” (p. 52). As the Founders demonstrated through their support for postal subsidies, for example, government has an active role to play in the proliferation of such goods. Today, governments may have an obligation to subsidize networks or services that have become a necessity rather than a choice (Drushel, 2011). More importantly, policy makers have an obligation to ensure that the journalistic and news reporting functions of mass media are preserved as a check on corporate and governmental power. As Jarvis (2013) argues, the power of incisive journalism to stem the tide toward secrecy and press powerful institutions to abide by the principle of openness “is all that can restore trust in government and technology companies.”

An expansion of what MacKinnon (2012) calls “the digital commons” also requires an articulation of universal principles by which corporations, governments, activists, journalistic organizations, and the public can envision, critically assess, and respond to changes in the digital environment (p. 15). In 2011, for example, the Dynamic Coalition on Internet Rights and Principles published a Charter of Human Rights and Principles for the Internet that outlines ten principles including the rights of accessibility, expression and association, privacy, and security (MacKinnon, 2012, pp. 240–241). Lori Andrews (2013) articulates similar principles in her proposal for a Social Network Constitution (p. 189). MacKinnon (2012) argues that such legal frameworks, in conjunction with innovative structures supporting corporate accountability, may provide a bulwark against coercive data collection strategies and ensure that the emerging digital environment properly represents the “consent of the networked” (p. 250).

If the metaphor of the lively, diverse, and accessible coffeehouse is always a counter-factual ideal, it is one worth pursuing nevertheless. Rather than acquiescence to rhetoric about the ultimate beneficence of technologies or the savvy entrepreneurs who produce them, that pursuit requires a persistent and collective struggle. The ethics of social media cannot be reduced to a question of personal conduct, but must call into question the very technologies, legal frameworks, and organizational structures that constitute the networked environment within which citizens pursue their personal, social, and political goals. Crucially, that environment is not yet
fully formed; but as its adolescence passes, efforts to reform its character will become increasingly difficult. In articulating the story of coercion, consent, and the struggle for social media, a primary charge of the coming generation of digital natives is thus to aid the formation of a mature social media environment—an ethically responsive and economically sustainable architecture of human flourishing.

NOTES

1. An earlier version of this chapter appears in Explorations in Media Ecology (Healey, 2014). This version has been updated to include relevant developments in cited examples, updated bibliographic citations, and minor editorial changes. Permission to re-publish granted by Explorations in Media Ecology on July 26, 2019.

2. Facebook, for example, faced boycotts in 2013 for its failure to monitor misogynous content.

3. For example, Kevin Kelly (2010) faults Amish communities for undermining the “optimization of choice” (n.p.).

REFERENCES


Drushel, Bruce E. (2011). “‘I’m Here to Tell You It’s OK.’: The FCC Chairman, Digital TV, and Lying to the Government.” In Bruce E. Drushel and Kathleen German (Eds.), The Ethics of Emerging Media: Information, Social Norms, and New Media Technology (pp. 119–134). New York: Continuum.


