Keen and Jarvis on Social Media Privacy and Connectivity

Posted on April 4, 2018

View this essay online:
https://academic-master.com/keen-and-jarvis-on-social-media-privacy-and-connectivity/

Introduction

Andrew Keen's "Sharing Is a Trap" and Jeff Jarvis's "Get Over It" represent two competing ways of understanding digital life. Keen fears that platforms built around constant disclosure weaken privacy, independence, and the protected space in which a person can think or change without being watched. Jarvis argues that openness can create knowledge, community, accountability, and practical help, and he warns that privacy claims can be used to block beneficial sharing. Their disagreement remains valuable because both authors identify a real human need. People require privacy to develop identity, preserve dignity, and protect themselves from misuse of personal information. They also require connection, communication, and access to shared knowledge. The central problem is therefore not whether society must choose privacy or connectivity. It is how individuals and institutions can distribute the benefits and risks of visibility fairly. The social-media environment that followed the authors' 2011 essays makes this question even more complicated. Platforms now collect behavioral data at a scale most users cannot see, automated systems infer sensitive characteristics, employers and governments can search old posts, and recommendation algorithms influence what people encounter. At the same time, online networks help families maintain relationships, patients find communities, social movements document injustice, and researchers or educators collaborate across distance. A balanced analysis supports Keen's insistence that privacy is a condition of freedom while accepting Jarvis's argument that voluntary openness can produce public value.

Keen's Warning: Visibility, Permanence, and Unequal Power

Keen's argument is strongest when he treats visibility as a form of power rather than a harmless social habit. He invokes Jeremy Bentham's Panopticon and Michel Foucault's observation that "visibility is a trap" to explain how people modify behavior when they believe they may always be observed. Social media extends this problem because users do not know exactly who will see a post, how long it will remain available, what later context will surround it, or what inferences will be drawn from it. A photo shared with friends can be copied, searched, combined with location data, or interpreted by an employer years later. The person who disclosed the information may have

technically clicked “agree,” but meaningful consent is doubtful when terms are complex and participation is socially necessary. Keen is also right that constant performance can blur the boundary between living and presenting a life. Users may select moments that support a desirable identity, compare themselves with edited images, or feel pressure to turn grief, relationships, parenting, and political belief into public content. Privacy provides more than secrecy; it offers room for experimentation, forgiveness, intimacy, and disagreement without permanent judgment (Jarvis).

Modern data practices strengthen Keen’s concerns. Platforms can collect clicks, pauses, contacts, device identifiers, search behavior, and location, while advertising systems connect information across services. Even when a user avoids posting sensitive details, data analysis may infer interests, health concerns, political attitudes, or personal relationships. The harms are not distributed equally. A wealthy professional can sometimes recover from exposure or pay for legal help, whereas a domestic-violence survivor, undocumented person, religious minority, teenager, or worker in a precarious job may face greater consequences. Children cannot fully understand the future effects of family “sharenting,” and biometric data cannot be replaced like a password. Privacy regulation therefore cannot rely only on individual settings. It should limit unnecessary collection, require clear purpose and retention rules, secure stored information, restrict harmful secondary uses, and give people practical rights to access, correction, deletion, and appeal. Keen sometimes writes as though social sharing itself destroys authenticity, but his deeper point is persuasive: freedom is weakened when participation requires surrendering control to institutions whose incentives depend on surveillance and engagement.

Jarvis’s Defense: Openness, Community, and Public Value

Jarvis argues that fear of exposure can obscure the gains created by openness. His personal account of discussing illness illustrates how sharing can encourage others to seek care, reduce isolation, and build communities around experiences once treated as shameful. This argument extends to many areas. Patients exchange practical knowledge about rare conditions, marginalized people find language for their identities, families maintain relationships across borders, students collaborate, witnesses publish evidence, and citizens organize disaster relief or political action. The value is not simply the quantity of information. Public disclosure can change what society recognizes as a common problem. Testimonies about harassment, discrimination, disability, mental illness, or caregiving may challenge silence and create pressure for institutional reform. Jarvis is also correct that privacy can be invoked selectively. Powerful organizations sometimes demand secrecy to avoid scrutiny, and public officials may describe legitimate accountability as an invasion of privacy. Transparency requirements for governments, corporations, research, and campaign finance can protect citizens rather than expose them (Keen).

However, Jarvis’s claim that people should “get over” privacy is too broad because openness is

beneficial only when it is voluntary and informed. The person sharing a medical experience may gain community, but that does not justify a platform selling health-related inferences or an insurer using them unfairly. A whistleblower's disclosure of institutional misconduct is different from the publication of a private individual's address. Openness also creates context collapse: information intended for one group reaches another audience with different assumptions. Jarvis tends to describe sharing as a transaction among people, while contemporary platforms mediate that transaction through ranking systems, advertising markets, and content moderation. The user who receives social support may simultaneously provide data that strengthens commercial profiling. Connectivity can therefore empower and exploit at the same time. The proper response is not to reject Jarvis's optimism but to add conditions: people must understand the audience, retain meaningful control, and have alternatives when they do not wish to disclose.

A Better Framework: Contextual and Accountable Sharing

The disagreement between Keen and Jarvis becomes more productive when privacy is understood as contextual control rather than absolute concealment. People routinely share different information with doctors, friends, employers, teachers, banks, and the public. A privacy violation occurs when information moves beyond the context in which it was reasonably provided or is used for a purpose that changes the relationship. A patient expects a physician to record symptoms for treatment, not to publish them for entertainment. A student may post a joke for classmates without intending it to become part of an automated employment profile. Contextual privacy recognizes that sharing and privacy are compatible: a person can disclose to a chosen community while resisting unlimited distribution (Nissenbaum).

Responsibility is shared among users, platforms, governments, schools, employers, and researchers. Individuals should use strong authentication, review audiences, avoid exposing other people without consent, and recognize that deletion may not remove copies. Schools should teach media literacy as civic education, including algorithmic influence, misinformation, digital consent, and the economic model behind "free" services. Employers and universities should avoid judging applicants through decontextualized searches. Platforms should minimize collection, make privacy defaults protective, separate essential service from advertising consent, explain recommendation systems, and provide effective remedies for harassment, impersonation, and non-consensual imagery. Governments should protect freedom of expression while regulating deceptive data practices and discriminatory uses. Transparency should apply most strongly to institutions that exercise power, while privacy protection should be strongest for individuals who have less capacity to defend themselves (Federal Trade Commission).

Another limitation in both essays is their tendency to imagine a single user. People do not enter social media with equal bargaining power or the same purpose. A public official, a teenager, an activist

using a pseudonym, and a small business may reasonably choose different levels of visibility. Cultural expectations also matter: openness can be celebrated as authenticity in one community and experienced as dangerous exposure in another. Design should support this diversity through separate audiences, temporary sharing, pseudonymous participation where lawful, and clear warnings when information may become public or searchable. Data portability and interoperability can reduce dependence on one platform, while independent oversight can test whether privacy promises match actual practices. Research access should also protect users; public availability does not automatically make posts ethically free for unlimited collection. These examples reinforce a principle missing from the original debate: the benefits of openness should be evaluated together with who controls the infrastructure, who receives the value, and who bears the risk.

Conclusion

Keen and Jarvis each capture one side of digital life. Keen correctly warns that permanent visibility, commercial surveillance, and social pressure can diminish freedom and authentic self-development. Jarvis correctly shows that openness can create knowledge, solidarity, care, and democratic accountability. Their positions become misleading only when treated as absolute. Privacy is not hostility to community, and sharing is not automatically surrender. The ethical goal is meaningful choice within systems that do not punish people for protecting themselves or exploit them when they disclose. A humane digital environment would allow individuals to decide what becomes public, preserve the possibility of changing over time, and require powerful institutions to explain how they collect and use information. Connectivity should expand human relationships without making every relationship a source of data extraction. In that framework, privacy and openness are not enemies; both are necessary conditions for trust.

Works Cited

Jarvis, J. (2011). Get over it. *Wired*.

Keen, A. (2011). Sharing is a trap. *Wired*.

Federal Trade Commission. Protecting consumer privacy and security. https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.