International Journal of Communication 17(2023), 7203–7223 1932–8036/20230005

Outcomes and Affordances: Examining Why People Use Encryption

SHANNON M. OLTMANN♦
University of Kentucky, USA

This project examined the use of encryption actively enabled by everyday users, such as encrypting one's hard drive or e-mail. Ninety-six respondents (mostly American males) were interviewed via telephone, e-mail, and instant messaging. Respondents provided unique insights into concerns about data collection and analysis. The findings indicate that encryption's affordances include inaccessibility and unreadability. Outcomes from these affordances include security, data integrity, anonymity, preventing self-incrimination, stopping surveillance, privacy, and freedom of speech. Respondents were less focused on the affordances of encryption, instead primarily thinking about their desired outcomes. This work argues that future scholarship should consider both affordances and outcomes when analyzing why people use particular technologies and platforms.

Keywords: encryption, affordances, privacy, outcomes, civil liberties

The literature on affordances is well-established, especially with respect to social media. Researchers have studied the relational aspects between humans and technology with particular attention to what is afforded by the technology, focusing on the imagined (Nagy & Neff, 2015) or perceived action possibilities. These have been mapped, critiqued, and analyzed; however, less attention has been paid to the *outcomes* of various affordances, despite that users are likely using technology to produce certain results. Although Evans, Pearce, Vitak, and Treem (2017) refined the distinctions between features, affordances, and outcomes, few have subsequently used this approach to study the relationships between affordances and outcomes. Nonetheless, we think that a focus on outcomes can tell us something valuable about how users think about and employ various technologies.

In this project, we study encryption as a technological *feature*, a window into (re)considering affordances and outcomes. Communication and information researchers have long wondered at the lack of widespread adoption of encryption (e.g., Orman, 2015). Encryption has often been decried as difficult to understand and implement for the average (nontechnically skilled) user. Although encryption is increasingly implemented "automatically" in the background (such as in WhatsApp, online banking, and the https protocol), its *active* adoption by users remains relatively low (Dencik & Cable, 2017). Here, we refer to users who take active steps to encrypt their hard drives, e-mail, texts, Internet traffic, and so on (see Costa, 2018). Presumably, those who take explicit action to encrypt are doing so for particular ends—that is, for

Shannon M. Oltmann: shannon.oltmann@uky.edu
Date submitted: 2023-03-13

particular *outcomes*. Thinking about outcomes of technology use can shed further light on technological affordances, illuminating how technologies are understood and used.

One example of an outcome is privacy (Evans et al., 2017). Different technologies affect privacy in various ways, either enhancing or reducing privacy. Affordances of these technologies affect the outcome of privacy. This project focused on actively enabled encryption as a way to find respondents who were highly concerned about privacy; in turn, these individuals were better positioned to describe the problems with data collection and analysis in nuanced, complex ways, including adding non-American voices to the mix.

In this research project, 96 respondents (mostly male and from the United States) were interviewed about encryption, privacy, and related aspects of using this technological tool. The respondents were interviewed via telephone, e-mail, direct message, and chat applications (the interview mode was selected by each respondent). In their interviews, respondents discussed two affordances of actively enabled encryption: inaccessibility of data and unreadability of data. They also reported a number of outcomes: security, data integrity, anonymity, preventing self-incrimination, stopping surveillance, privacy, and freedom of speech. In general, respondents focused more on the outcomes they desired and less on the affordances that produced the desired outcomes.

This study proceeds with background information about online privacy, encryption, and affordances. The subsequent section discusses the methods used, followed by results and discussion. The overrepresentation of American males is one limitation of this study, though the inclusion of international respondents illuminated some unique concerns.

Literature Review

Online Informational Privacy

Online informational privacy is a complex concept, but at its heart is "the desire to keep personal information out of the hands of others" (Cho, Rivera-Sanchez, & Lim, 2009, p. 397). Braunlich and colleagues (2021), in their development of an interdisciplinary privacy and communication model, noted that two concepts common across most definitions of privacy are the limitation of access and control of access (p. 1445) to information. This harkens back to Westin's (1967) foundational definition of privacy: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7; see Bannerman, 2019, for a revision of Westin's work).

As the Internet has developed, it has increasingly become focused on the collection and analysis of users' data by both corporate and governmental institutions (Couldry & Yu, 2018; Dencik & Cable, 2017; Hart, Jin, & Feenberg, 2014; Landwehr, Borning, & Wulf, 2021; Winseck, 2002), to the point that we now live in a "surveillance culture" (Lyon, 2017; see also Dencik & Cable, 2017; Zuboff, 2015). Rubel and Biava (2014) stated "there is substantial concern about privacy in light of technological advances, great sharing of information via social networks, and increased power of state and nonstate actors to collection information about individuals" (p. 2422; see also Kubitschko, 2015; Vitak et al., 2023). This datafication of individuals occurs mostly in the background of Internet use and mostly without explicit permission from individuals. It

has become more visible in the past several years with the Snowden revelations (occurring in 2013), the Equifax data breach (2017), and the Cambridge Analytica scandal (2018), all of which revealed that a great deal of user data is being collected and analyzed (see Kalmus, Bolin, & Figueiras, 2022; Lyon, 2017; Rogers & Eden, 2017).

Online government surveillance creates chilling and deterrence effects and can spur people to change their privacy settings (Mak, Koo, & Rojas, 2022), move to other platforms (Johns, 2021), or participate less in online debate and exchange of ideas (Stoycheff, Liu, Xu, & Wibowo, 2019). Pew Research Center (2019) reported that about eight in 10 Americans felt a lack of control over the data the government collects and the data that companies collect; majorities were also concerned about how the data were used and felt that risks of data collection outweighed the benefits.

These issues have led researchers to develop concepts such as privacy paradox and privacy calculus. The paradox is that people state they value privacy, but routinely and consistently act in contravention of this statement (i.e., by sharing personal information on social media; see, e.g., Taddicken, 2014). For example, only 30% of Americans took active steps to shield their data when online (Pew Research Center, 2018). Privacy calculus is a more nuanced analysis, positing that individuals calculate how much information to share or withhold. In other words, "concerns about online privacy represent how much an individual is motivated to focus on their control over a voluntary withdrawal from other people or societal institutions on the Internet" (Dienlin, Masu, & Trepte, 2023, p. 4; see also Bol et al., 2018; Lauriano, 2023).

Further, privacy and data control have "become inextricably linked to problems of personal choice, autonomy, and socioeconomic power" (Acquisti, Brandimarte, & Loewenstein, 2015, p. 509; see also Andersen, Boge, Danholt, & Lauritsen, 2018). Other researchers have noted that "online privacy can never be assured and that any privacy expectations should be tempered with caution, knowledge and personal control" (Martin, Rice, & Martin, 2016, p. 502). In fact, Kubitschko (2015) argued that "technological developments in data processing pose serious challenges to societies as they destabilize the delicate balance between privacy, security, autonomy, and democratic rights" (p. 81; see also Silverman, 2017; Zuboff, 2015).

When people do have strong concerns about online privacy, they may respond by enacting privacy-enhancing measures (Dienlin et al., 2023; Lauriano, 2023). For example, Winseck (2002) reported that privacy-enhancing technologies such as encryption and cryptography are designed to give people control over their personal information. Likewise, Jardine (2018) and Chen, Jardine, Liu, & Zhu (2022) determined that most users of Tor are likely using it to protect their privacy, not to access illicit content or drugs (see also Siuda, Nowak, & Gehl, 2022, who describe the cultural imaginaries of the darknet as contested).

Encryption

One tool to protect privacy online is encryption—that is, the conversion of plaintext, easily readable data or messages into an enciphered form or cipher text, using complex algorithm functions (see National Academies of Sciences, Engineering, and Medicine, 2018, or Orman, 2015, for a "gentle" introduction to

encryption). The strength of encryption is based on these complex functions,[1] which are currently computationally infeasible to solve; the mathematics involved make the message essentially unreadable unless one has the "key" to "unlock" the encryption.

Encryption is used increasingly across technology applications to provide enhanced security and privacy (Hosein, 2017; Landwehr et al., 2021; National Academies of Sciences, Engineering, and Medicine, 2018); for example, messaging applications such as WhatsApp use encryption to protect the content of messages. Indeed, many argue that encryption is essential for modern communication, commerce, and national security (e.g., Hart et al., 2014). Although some encryption happens "behind the scenes," requiring no action on the part of the user, there are other sorts of encryption that do require explicit action to be taken by the user; examples include encrypting one's hard drive, e-mail, or Internet traffic (Gliksberg, 2017, makes a similar distinction). In the past, encryption has been perceived as difficult to employ (e.g., Bai, Pearson, Kelley, & Mazurek, 2020; Orman, 2015; Sheng, Broderick, Koranda, & Hyland, 2006; Wu & Zappala, 2018).

According to the literature, encryption is used for various reasons; privacy and confidentiality are often seen as the primary motivations. Additional reasons include "data integrity (the prevention and detection of unwanted data manipulation), authentication (the identification of sender and recipient), and nonrepudiation (the prevention of entities from denying previous commitments or actions)" (Vagle, 2015, p. 117). Kozinski (2015) argued that the main outcome of encryption was anonymity. Some individuals have further argued that encryption protects freedom of speech, because what one says or does online cannot be connected to one's real-life identity (Karlstrom, 2014). Yet we know relatively little about how and why people actively choose to use encryption, despite the increasing importance of this technological tool.

Affordances

Because we know little about motivations for using encryption, an affordances lens can provide us with structure for exploring this question. Affordances have been frequently used to describe the relational interaction[2] between humans and technology (e.g., Aziz, 2022; Bucher & Helmond, 2017; Evans et al., 2017; Faraj & Azad, 2012; Freeman & Neff, 2023; Kim & Ellison, 2021; Pagh, Skovhoj, & Lai, 2022). Most descriptions of affordance start with Gibson (1986), noting that affordances are perceived action possibilities in the environment. Evans and colleagues (2017) emphasize that affordances "emerge in the mutuality between those using technologies, the material features of those

[1] Though people may consider encryption to be a recently developed technique, it has in fact existed for centuries (in various forms). For example, Singh (1999) and Vagle (2015) described the efforts of Mary, Queen of Scots, to communicate with her supporters in the 16th century using encryption, and Edgett (2003) noted that the U.S. founding fathers encrypted messages to ensure confidentiality.

[2] Kini, Pathak-Shelat, and Jain (2022) note that "new media studies and communication scholars have conceptualized affordance as perceived, communicative, imagined, vernacular, relational and multilayered, and platform sensitive" (pp. 1575–1576). Although Gibson (1986) emphasized the relational aspects, this has been expanded and complicated by subsequent scholars.

technologies, and the situated nature of use" (p. 36; see also Fu & Zhang, 2019). Importantly, affordances can "request, demand, allow, encourage, discourage or refuse certain actions," illustrating the full range of potentialities (Lee, Liang, Cheng, Tang, & Yuen, 2022, p. 1701; see also Davis & Graham, 2021; Haciyakupoglu & Zhang, 2015). Costa's (2018) focus on affordances-in-practice emphasizes the importance of the "situated practices of usage" (p. 3645). Indeed, the abilities and skills of the user are an important aspect of enacting affordances; not every actor is capable of utilizing every affordance (nor does every user necessarily perceive or want to use every affordance available; Anderson & Roby, 2017; Ballucci & Patel, 2022; Bimber & Gil de Zuniga, 2020; Costa, 2018; Denegri-Knott, Jenkins, & Lindley, 2022; Freeman & Neff, 2023; Fu & Zhang, 2019; Meisner & Ledbetter, 2020; Pagh et al., 2022; Tandoc, Lou, & Min, 2019). Technologies may have multiple affordances, and affordances may have multiple outcomes (Evans et al., 2017; Faraj & Azad, 2012; Karahanna, Xu, Xu, & Zhang, 2018; Pearce & Malhotra, 2022).

From the vast literature on affordances, two points are particularly salient. First is the distinction between features, affordances, and outcomes, developed by Evans and colleagues (2017) to further refine the conceptualization of affordances. Features, in this framework, are static technical aspects. Affordances invite behaviors and describe the relation between the user, the object, and its features. Outcomes are the results of enacting affordances; "affordances invite behaviors and other outcomes but are not the outcome itself. An outcome need not be an action but needs to be connected with the goals of the actor" (Evans et al., 2017, p. 40). Evans and colleagues (2017) usefully used recordability as an example: the built-in camera on a smartphone is the feature, recordability is the affordance, and recording, say, a human rights violation is an outcome (pp. 39–40). Using encryption to disguise one's Internet traffic (a *feature* of certain VPNs) has an *affordance* of unreadability (the data cannot be read by outside parties) and several possible *outcomes*, including enhancing freedom of speech. Similarly, Faraj and Azad (2012) usefully distinguished between features ("technical attributes and ways of working inscribed in the artifact by technology designers") and affordances ("possibilities of using select features or combinations of features in a way meaningful to the user's goals, abilities, and lines of action"; p. 254; see also Denegri-Knott et al., 2022).

The second salient point is developed by Nagy and Neff (2015) in their depiction of "imagined affordances." These "emerge between users' perceptions, attitudes, and expectations; between the materiality and functionality of technologies; and between the intentions and perceptions of designers" (Nagy & Neff, 2015, p. 1). The potential actions that users imagine can be undertaken with a particular technology are imagined affordances (even if those affordances are not what designers intended). Taken with the first point, this means that users imagine what can be done with certain *features*, then enact the *affordances* that (they think) will yield the *outcomes* they desire.

Much of the affordance literature focuses on the affordances of particular features, technologies, and platforms, often social media platforms. However, the literature that considers the *outcomes* of using affordances is scarce. Yet, if people use affordances to result in particular outcomes (as they surely do), then the (potential) outcomes are significant. Focusing on outcomes can help us identify new, different, or unexpected affordances. It can help us conceptualize the mechanics of just how affordances are perceived, conceptualized, and enacted. Outcome-based research can also better examine why people use particular

technologies or platforms (for a different, but related approach, see Denegri-Knott et al., 2022, for their examination of "goals" that motivate technology use).

This project therefore examines the affordances and outcomes of encryption—in particular, encryption that is actively engaged by users (such as choosing to encrypt one's hard drive, e-mail, and/or Internet use). Applying the affordances framework, the extant literature describes the affordances of encryption as the unreadability and inaccessibility of data; the anticipated outcomes include privacy, confidentiality, data integrity, authentication, nonrepudiation, anonymity, and freedom of speech.

Methods

To investigate how individuals use encryption, this project sought respondents who actively enabled encryption, such as encrypting e-mail, hard drives, and/or Internet traffic. (Passively enabled encryption did not qualify.) The data for this project were collected via qualitative interviews. Subjects were recruited in multiple ways. First, recruitment messages were shared on relevant listservs, such as the listserv for the Association of Internet Researchers and on computer developer public forums. Second, recruitment posts were made on the researcher's social media accounts (such as Facebook and Twitter). Third, recruitment messages were also posted in relevant Craigslist discussion fora (such as "comp"). Recruitment messages were posted in relevant subreddit threads (such as r/privacy and r/crypto). Finally, some subjects were recruited via snowball sampling: some respondents forwarded the recruitment message to other individuals. All recruitment efforts and interviews occurred using English only; a total of 96 respondents were recruited and successfully interviewed. These methods are similar to those used in Gallagher, Patil, and Memon (2017), who recruited Tor users via Reddit, Craigslist, and university mailing lists (p. 387).

Interviewees selected the format that best suited them: encrypted e-mail (n = 36; median word count 1,385), Reddit private message (n = 34; median word count 1,217), telephone (n = 19; media word count 3,778), unencrypted university e-mail (n = 3; median word count 2,689), Twitter direct message (n = 2; median word count 1,267), and encrypted chat applications (n = 2; median word count 1,810); the total corpus was 178,807 words (average word count across all respondents was 1,863) or 333 single-spaced pages. All interviews were transcribed (if necessary) and converted to Word documents and then uploaded into Dedoose for sentence-level coding and analysis.

Each subject was asked for his or her gender and nationality (see Table 1 and Table 2). The respondents were overwhelmingly male (n = 70), with only four females and one identifying as genderqueer. Nearly a quarter of participants chose to not identify their gender (n = 22). Respondents were also asked about their nationalities. About 39% were American (n = 39), with the next most-represented nationalities being British (n = 5), Australian (n = 3), and Dutch (n = 3). Approximately one-third of respondents did not identify their nationality (n = 31). Pseudonyms were selected from an online random name generator.

Table 1. Gender of Respondents.

Gender	Number of participants	Pseudonyms of participants
Male	70	Abdias, Arnie, Austin, Benito, Biff, Blake, Bob, Brandon, Cameron, Carlos, Clive, Darrin, Dawson, Delano, Delbert, Derrick, Dominik, Donnie, Duke, Earl, Edric, Elliot, Eric, Florencio, Frederick, Garth, Geordie, Gerald, Hamilton, Harry, Harvey, Horatio, Humphrey, Immanuel, Ivan, Jack, Jason, Jerry, Jordan, Kade, Kyle, Lamont, Leon, Lon, Lucio, Luke, Mervin, Mike, Montgomery, Neville, Newton, Nic, Ollie, Oswald, Phil, Quentin, Rafe, Reuben, Robbie, Roger, Saul, Seymour, Sheldon, Terrence, Todd, Virgil, William, Winslow, Xavior, Zander
Female	4	Anissa, Cosette, Skye, Vickie
Genderqueer	1	Tracey
Did not specify	23	Andie, Bailey, Carson, Charley, Chris, Dakota, Devin, Everett, Frankie, Harlow, Jeno, Jody, Joey, Lesley, Lindsey, Marty, Nat, Pip, Robin, Sal, Sammy, Tam, Taylor

Table 2. Nationality of Respondents.

Nationality	Number of respondents	Pseudonyms of respondents
United States of America	39	Abdias, Arnie, Austin, Blake, Bob, Cameron, Carlos, Dawson, Delbert, Donnie, Earl, Edric, Elliot, Eric, Florencio, Frederick, Garth, Gerald, Harry, Harvey, Horatio, Humphrey, Ivan, Jason, Jordan, Kyle, Lamont, Leon, Lon, Montgomery, Neville, Newton, Ollie, Rafe, Roger, Saul, Terrence, Vickie, Virgil
British	5	Derrick, Duke, Geordie, Mervin, Tracey
Australian	3	Everett, Jack, Winslow
Dutch	3	Benito, Phil, Skye
Canadian	2	Lucio, Dominik
Polish	2	Kade, Quentin
Russian	2	Immanuel, Xavior
Swedish	2	Oswald, William
Brazilian	1	Seymour
Chinese	1	Mike
Filipino	1	Robbie
Finnish	1	Hamilton
Indian	1	Nic
Nigerian	1	Anissa
Spanish	1	Zander
Swiss	1	Reuben

Did not specify	32	Andie, Bailey, Biff, Brandon, Carson, Charley, Chris, Clive, Cosette, Dakota, Darrin, Delano, Devin, Frankie, Harlow, Jeno, Jerry, Jody, Joey, Lesley, Lindsey, Luke, Marty, Nat, Pip, Robin, Sal, Sammy, Sheldon, Tam, Taylor, Todd

To aid in data analysis, national "Global Freedom Scores" were examined for the countries from which respondents originated. These scores rate "people's access to political rights and civil liberties" and yield three degrees of freedom for a country's citizens: free, partly free, or not free (Freedom House, 2022, para. 1). Based on these data, respondents from Russia (Immanuel and Xavior) and China (Mike) were located in "not free" nations; respondents from the Philippines (Robbie), India (Nic), and Nigeria (Anissa) were located in "partly free" nations; and the other respondents (from the United States, Great Britain, Australia, The Netherlands, Canada, Poland, Sweden, Brazil, Finland, Spain, and Switzerland) were in "free" nations. It is important to note that we do not know the relative freedom experienced by 32% of the respondents because they did not specify their nationality. In addition to these global freedom scores, the history of particular nations may be important. For example, respondents from European nations that were controlled by the Nazis/Axis powers during World War II (such as The Netherlands, Poland, Finland, and Spain) may have unique perspectives on government data collection; likewise, those from nations with authoritative pasts (namely, Russia, Brazil, China, the Philippines, and Nigeria) may have valuable insights.

Affordances

From the data, two affordances clearly emerged: the inaccessibility of data and the unreadability of data. Encryption—the affordance of *inaccessibility*— "allows me to have control over my electronic stuff, same as locked doors, safes, safety deposit boxes etc [sic] allow me to have control over my physical assets" (Everett, Australia); in other words, the feature of encryption affords data that are inaccessible to others. Saul (United States) added, "probably, the ability to keep unwanted parties out of systems, and systems is very broad. That could be, you know, a small file or a large computer, but that's kind of what encryption allows me to do." Immanuel (Russia) said he encrypted because of "governments seeking to censor free speech, [and] businesses betting on mining users' data . . ." which he saw as particularly insidious in his native country. With encryption, the data exist but are not accessible by others; it is essentially locked away through the mechanism of complex cryptography.

The second affordance, *unreadability*, protects data somewhat differently. For example, Nat (did not specify nationality) said they began using encryption "when I realized how incredibly simple it is to take a used hard drive and extract enough data off of it to ruin someone's life." In contrast, encryption affords data that are unreadable (a cipher text), as Xavior (Russia) noted: "Encryption scrambles a file to where anyone without the key can't decipher what it was." Cosette (did not specify nationality) added that, "When I use encryption, I am somewhat protecting my information in the sense that the information is a harder target to crack, especially for opportunistic or less sophisticated attacks." The affordance of unreadability means that the cipher cannot be read without the key, so the data exist but are meaningless. Zander (Spain) said that encryption, by making data unreadable, protected dissidence and hence democracy:

> Dissidence is fundamental for the functioning of our political systems, and being constantly exposed to everybody's judgements would just destroy all new ideas. What could, indeed, a powerful enough state do, if they had the power to suppress anyone who thought differently?

These two affordances yield several different outcomes, including security, data integrity, anonymity, stopping self-incrimination, preventing surveillance, confidentiality, privacy, and freedom of speech; while some of these were described in the previous literature about encryption, others were not. Different users sought different things from encryption, and most sought multiple outcomes; see Figure 1 for a depiction of the affordances and outcomes of encryption derived from the respondents.

Outcomes

These affordances of inaccessibility and unreadability afforded multiple outcomes for various users. In other words, as a result of using the feature of encryption, users obtained or gained the particular outcomes they were seeking. Most respondents focused on the outcomes of using encryption, rather than the affordances that led to the outcomes.

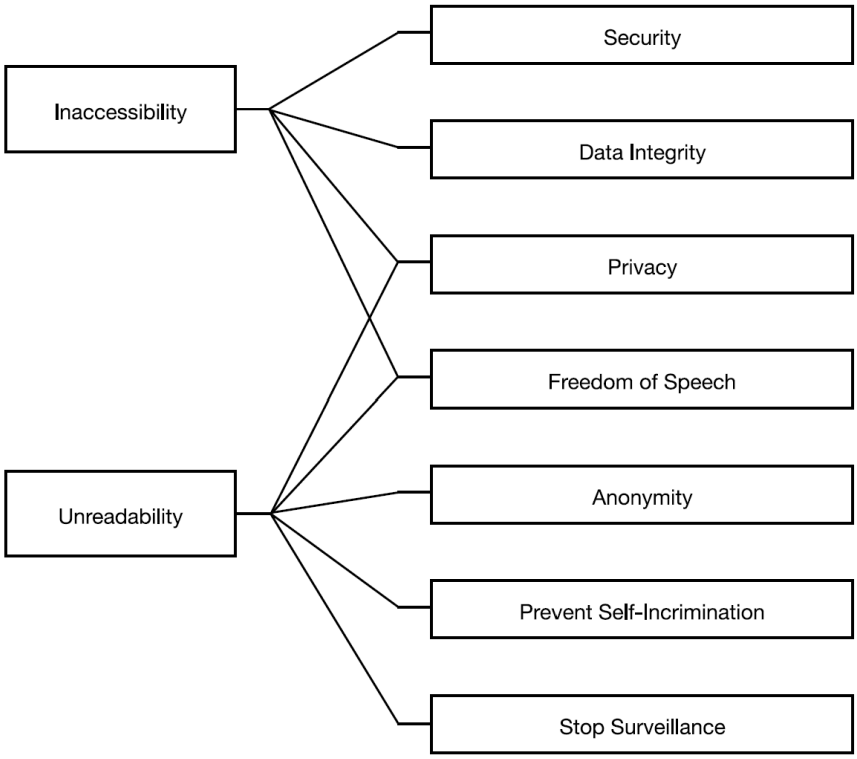

Figure 1. Relationship between affordances and outcomes.

Security

Fifty-two respondents (out of 96) mentioned security as an important outcome of using encryption. For example, Pip (did not specify nationality) said, "Encryption is the best way to ensure data security other than just not creating any data," and Todd (did not specify nationality) added, "It's a security measure so that my data is not at risk." Jack (Australia) explained that he used encryption because security was very important to him: "Security itself I value fairly highly, in that you can never have retroactive privacy or paranoia—only proactive. Once you've been 'burned,' it's too late to go back. For that reason, it's best to be vigilant from the beginning." He saw encryption as a way to increase his vigilance in this regard.

In their attempts to explain the importance of security, several respondents provided rough definitions. Lindsey (did not specify nationality) said, "I define security as having a reasonably strong belief that any data I encrypt will not fall in the wrong hands." Humphrey (United States) extended this:

> I believe everyone has a right to security, just like they have the right to free speech or privacy. Security is knowing that someone is not constantly monitoring your "find my iPhone" or scanning through every text, e-mail, note, or thought that becomes digital.

Earl (United States) suggested that security means "having your private items under your own control. You control what gets out. You control what is seen by others."

Data Integrity

Twenty-four respondents described the importance of data integrity as a reason for using encryption. Jeno (did not specify nationality) said, "digital signatures can ensure data integrity—that nothing was altered and the message or software that's signed is authentic (it helps in high-risk environments), or even every day where you want to avoid communication being intercepted and altered." Clive (did not specify nationality) noted that "people don't realize how valuable their data is. And I think they also don't realize how fragile, how unsecure their data is." Darrin (did not specify nationality) explained that, with encryption, people can:

> know who (a) sent it and (b) received it. And secondly, that the mail that you send is received complete and untouched and, for that matter, unread by persons unknown. It all has to do with delivering the message to the intended-intended recipient, intact, untouched, unread.

Part of data integrity, for these respondents, was ensuring who the sender and receiver were. For identity verification, Skye (The Netherlands) noted, "by digitally signing messages, you can be sure that they always come from the same person." This example demonstrates explicitly that the same feature can be perceived to have different outcomes by different people; Jeno (did not specify nationality), above, suggested that digital signatures ensured data integrity, while Skye (The Netherlands) saw them as a form of identity verification.

Anonymity

In this project, 22 respondents emphasized the importance of anonymity as an outcome of encryption. Sheldon (did not specify nationality) explained, "for me, it's all about anonymity. I think, pretty soon, everyone's going to realize that they need alternate egos, they need alternate lives." Zander (Spain) added that "sometimes it just feels good to be anonymous." These respondents used encryption to obfuscate their identities from other users and entities online.

Sometimes this was based on historical context; for example, Anissa (Nigeria) noted that her parents lived through World War II in France, and said, "I was told since my childhood of how the French govt [*sic*] decided to give the Jews to the Nazis and that what is allowed today might not be in some more [or] less distant future." From another Nazi-occupied nation, Hamilton (Finland) said, "Depending on the politicians in charge, being associated with specific political views, for example, could hamper my future work career." Likewise, Kade (Poland) added:

> Historically, governments don't have a particularly good track record, and [they] like going insane from time to time, and thus something like being persecuted, made easier by private information obtained through surveillance programs, for one's political leanings is not something completely outside the realm of possibility within the next 20 years.

Elliot (United States) added that, "I like to contribute my boring Internet traffic to Tor and Tails to make the network more usable for those who really need to be anonymous for personal safety." Along with several other users who voiced similar thoughts, Elliot (United States) believed that his obscured traffic added to the total amount of encrypted traffic, thus making it more difficult to pinpoint particular individuals. Another user, Vickie (United States), said, "that's the biggest [reason] why I definitely use it, the confidentiality that kind of exists. Having had an online stalker, like that really makes you want to hide your tracks."

Stopping Surveillance

Fifty-one respondents said they used encryption as a means of stopping or limiting surveillance. For example, Frankie (did not specify nationality) said, "I use encryption because I hate that governments think that I should be spied on and because I like to feel safely [*sic*]." Reuben (Switzerland) added, "Today, regardless of laws, your devices and transmission of data can be taken from you and looked at without permission. Encryption is how you make it more difficult for that data to be seen." Anissa (Nigeria) noted that, in her native country, "I had a friend cop tell me that he saw other cops from a tech division intercepting phone calls without needing any prior operation on the device." Her knowledge of authoritarian law enforcement surveillance led her to use encryption.

For many respondents, then, the worry was government collection, analysis, and misuse of data. If one prevents the government from collecting one's data, then no analysis or misuse can follow. Skye (The Netherlands) elaborated on the importance of making sure data were unreadable, based on her country's history with the Nazi occupation. She offered data about the high rate of Jewish deaths from The

Netherlands, attributed this to the "very fine records of its citizens" kept by the country, and concluded, "Mass collection of personal data is a danger to humanity. The very fact that the data exists, waiting to be exploited, is a Holocaust-sized stain upon mankind withing to happen. It is a ticking timebomb."

Rafe (United States) extended this argument, saying, "Encryption is the new check on power . . . it offers the opportunity for a greater fundamental check on power than anything else will in our increasingly digital world." Thus, encryption becomes not just a means of evading government surveillance but also a potential tool for opposing surveillance and government overreach. Blake (United States) emphasized that such protection against government surveillance is not just for a potential future of authoritarianism: "I do some human rights work, so I also train journalists and dissidents and other people on the proper use of strong crypto." Likewise, Zander (Spain) said:

> If we lived in a world where our every move (and literally every move, as technology is further diluting the boundaries between real and digital world) could be tracked, in a way which never forgets and never forgives, because computers have almost unlimited memory, will we ever take risks? It's proven that people behave different [*sic*] when they are being observed, so, where will our identities go?

Preventing Self-Incrimination

Nineteen respondents talked about encryption as a way to prevent potential self-incrimination. Neville (United States) said that the first time he used encryption was "because I had files that were incriminating," but since then he's used it for protecting all of his files and data, so now, he said, "I know soundly that the government or hackers aren't going to be able to access my personal information. I won't be put onto a list for having a certain political belief. My assets are safe. I can't be blackmailed." Mike (China) added, "I've seen digital information used against others countless times, so I fear the same thing."

Along those lines, Geordie (Britain) said, "If you can't operate in private, it's much more difficult to do unusual things without attracting criticism or persecution from others." These respondents used encryption to hide some of their data or online activity, for a number of reasons: They may be breaking laws or norms, they may be aiding others in doing so, or they feared that now-innocuous activities may become illegal.

Privacy

Eighty-three people discussed the importance of preserving privacy in relation to encryption. For these respondents, encryption was a way to protect their privacy. Both the inaccessibility and unreadability of affordances were discussed as ways to afford the desired outcome of privacy. In terms of inaccessibility, Derrick (Britain) said, "Privacy for me is the ability to determine what information/data are shared and where/who it goes to" and Newton (United States) added, "privacy is concerned with protecting information from being accessed by anyone."

Nat (did not specify nationality) said, "I started encrypting to keep personal stuff private." This respondent wanted to make some data unreadable, to protect their privacy. Jeno (did not specify nationality) added that he wanted to protect privacy by "securing my online communications or data against eavesdropping." Bailey (did not specify nationality) said that they use encryption as "just walls we build around our digital lives" to prevent others from reading and (mis)using our personal information. Some respondents were particularly worried about the United States's ability to track data, even if they were not American citizens. For example, Zander (Spain) said, "The vast powers of the NSA [National Security Agency] really scare me out, given that, in the wrong hands, they could do too much danger, posing and [*sic*] effective threat to democracy worldwide, even when I am not from the US." Phil (The Netherlands) added:

> I used to trust my own government until it became very clear they were working on their own dragnet surveillance bill . . . I don't trust a government that saves my data. The things they want to collect about me now are not illegal right now, but what about the future? I don't decide what's illegal, the government will.

As they were discussing their desired outcome of privacy, several respondents tried to provide definitions. For example, Chris (did not specify nationality) defined privacy as, "protecting a notion of the self. Just like people need respect and dignity, they need privacy." Quentin (Poland) took a different tack: "privacy is 'the ability to control the disclosure of information about me.' My privacy is respected when I can choose which personal information I share with others." Essentially, privacy is "keeping your personal data [and] personal information out of the hands of nosey people and nefarious people" (Ivan; United States). Sal (did not specify nationality) brought together the affordances of inaccessibility and unreadability in his definition of privacy: "having your information under your control. Privacy is the inability for anyone to look up and learn any and all about you that they desire."

Freedom of Speech

Finally, 35 respondents discussed freedom of speech as an outcome they sought from using encryption. Joey (did not specify nationality) said, "I also really like that I can actually say whatever I want to, and not even remotely have to think about how it looks, or if someone will try to use it against me in the future." Likewise, Montgomery (United States) said he uses encryption because of "the ability to communicate free from chilling effects." Respondents clearly noted that surveillance has a chilling effect on speech, to which they were opposed. They saw that encryption prevented surveillance, thus eliminating the chilling effect. Garth (United States) elaborated:

> Western civilization as we know it is not possible in the age of the Internet without near-universal application of strong cryptography. For example, democracy relies on the free exchange of ideas, and a government, which is beholden to its citizens. If the powerful folks are able to hear private speech, or decide what is and isn't acceptable speech, then those ideas are dead . . . Encryption is the only answer.

Dawson (United States) added, "Active censorship, in my opinion, significantly reduces the diversity of opinions, and I believe that everyone should have access to a wide variety of information. How can they make informed decisions otherwise?"

Discussion

As described above, respondents viewed encryption as a feature or tool, a means to their desired ends. Seventy respondents explicitly described encryption as a tool, in fact. Roger (United States), for example, said, "Encryption, like a knife, is a tool. There are some people that do bad things with it, but for the most part it benefits the world." Based on this data, encryption is a technological feature that has two primary affordances, inaccessibility and unreadability. Inaccessibility means that the data or information that has been encrypted is not accessible; others are prevented from opening or finding it. Unreadability means that the data that *are* seen becomes a cipher text, not able to be read by humans or machines.

These two affordances yield several outcomes as identified by the study's respondents. The outcomes include security, data integrity, anonymity, preventing self-incrimination, stopping surveillance, protecting privacy, and freedom of speech. For most of the respondents, encryption's affordances were less central to their thinking and usage than *outcomes*. They had desired endpoints or goals, which motivated their utilization of encryption. In other words, they were more focused on the outcomes (what they wanted to achieve) than the affordances (how they achieved these outcomes). Thus, current scholarship's extensive focus on affordances of technologies may be somewhat misplaced if we do not also consider the outcomes (or, per Denegri-Knott et al., 2022, goals) that the various affordances yield. Most users (at least in this study) think and care more about the outcomes than the affordances, so outcomes should be more thoroughly studied and analyzed. Furthermore, a focus on outcomes may provide new insights into how we conceptualize and describe affordances. Further work on affordances should explicitly consider and report on outcomes as desired and sought by technology users.

This research used extensive data collection, across 96 interviews, to study affordances and outcomes of encryption. We discovered that respondents focused primarily on outcomes and generally left the affordances implicit in their thought process about selecting and using various encryption tools. Respondents were not asked explicitly about either affordances or outcomes; these emerged organically from the discussion about use of encryption. The data set included a preponderance of males and U.S. citizens, which may affect its generalizability. We were unable to reach many women; it is unclear whether this is because of the choice of recruitment approaches, whether relatively few women use encryption, or some other reason. It is possible that women do use encryption more often than indicated in these data, perhaps for securing home and social communications. This is an avenue ripe for future work.

In addition, because the respondents were all privacy-conscious and cautious individuals, some were not very forthcoming during their interviews. The median word count across all interviews was 1,863, though some interview modes (such as telephone and unencrypted e-mail) yielded far more words, on average, than other modes; this variability may be a weakness. Future work looking at encryption or other privacy-related technologies should consider ways to alleviate the privacy-related concerns of respondents.

At the same time, however, focusing on technologically skilled, privacy-conscious individuals allows us to uncover nuanced understandings of data collection and analysis. These respondents thoughtfully articulated several distinctive aspects to the broad topic of "privacy," such as different concerns about how data collection could impinge on civil liberties.

The international scope of respondents offered some unique insights. Several respondents from nations occupied by the Nazis in World War II explicitly referenced data collection in connection with the Holocaust; they said that fear of a similar horror was part of their motivation for using encryption. Others from authoritarian states expressed similar caution about data collection, whereas some respondents from U.S.-allied nations voiced concern about American data collection in particular (perhaps in part because many multinational corporations and social media platforms are U.S.-based).

This work found that respondents focused on specific outcomes that were somewhat different than those suggested by the literature. Previous work described the outcomes of using encryption as privacy, confidentiality, data integrity, authentication, nonrepudiation, anonymity, and freedom of speech. However, concepts such as authentication and nonrepudiation were not explicitly valued as outcomes of encryption used by these respondents; rather, they specified security, data integrity, anonymity, preventing self-incrimination, stopping surveillance, privacy, and freedom of speech. Thus, security, preventing self-incrimination, and stopping surveillance are outcomes uniquely surfaced by this research. Of particular interest are privacy and freedom of speech, two fundamental civil liberties.

The research reported here suggests that technological affordances are imagined (Nagy & Neff, 2015) to enact some civil liberties, and then are used to do so. Although others have connected technology to human rights and civil liberties, this research describes the specific ways in which technology, affordances, and civil liberty outcomes are connected. Importantly, the National Academies of Sciences, Engineering, and Medicine (2018) noted, "The availability of encryption has come to be recognized as intrinsically bound with rights to privacy, free speech, freedom of association, and freedom of religion, collectively referred to as civil liberties or human rights" (p. 32). Their report goes on to argue that the protection of online manifestations of civil liberties is especially important in the information age. Similarly, Siuda et al. (2022) noted some depictions of the darknet (including encryption technologies) emphasize civil liberties such as freedom of speech and freedom from surveillance, though protection of such liberties may only be available to the technologically skilled (pp. 12–13).

Furthermore, the United Nation's Special Rapporteur on freedom of opinion and expression, in 2015, reported that encryption was fundamental in protecting freedom of expression (United Nations, 2015). Thus, the connection between encryption and human rights has long been recognized; this project helps to articulate that relationship in detail, using the affordances framework. This framework can be used to further investigate how civil liberties are protected, enhanced, or constrained through various technologies and platforms. In conclusion, this project suggests that study of encryption and other civil liberty-protecting technologies should be increased; in addition, the specific ways in which other technologies and platforms yield outcomes of protected civil liberties should be further studied.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. doi:10.1126/science.aaa1465

Andersen, L. B., Boge, A. R., Danholt, P., & Lauritsen, P. (2018). Privacy encounters in Teledialogue. *Information, Communication & Society, 21*(2), 257–272. doi:10.1080/1369118X.2016.1271904

Anderson, C., & Robey, D. (2017). Affordance potency: Explaining the actualization of technology affordances. *Information and Organization, 27*(2), 100–115. doi:10.1016/j.infoandorg.2017.03.002

Aziz, A. (2022). Affective networked space: Polymedia affordances and transnational digital communication among the Rohingya diaspora. *International Journal of Communication, 16*, 4073–4094.

Bai, W., Pearson, M., Kelley, P. G., & Mazurek, M. L. (2020). Improving non-experts' understanding of end-to-end encryption: An exploratory study. In *2020 IEEE European Symposium on Security and Privacy Workshops* (pp. 210–219). Genoa, Italy: IEEE. doi:10.1109/EuroSPW51379.2020.00036

Ballucci, D., & Patel, M.-G. (2022). Digital media 'changes the game': Investigating digital affordances impacts on sex crime and policing in the 21st century. *Information, Communication and Society*. Advance online publication. doi:10.1080/1369118X.2022.2113422

Bannerman, S. (2019). Relational privacy and the networked governance of the self. *Information, Communication & Society, 22*(14), 2187–2202. doi:10.1080/1369118X.2018.1478982

Bimber, B., & Gil de Zuniga, H. (2020). The unedited public sphere. *New Media & Society, 22*(4), 700–715. doi:10.1177/1461444819893980

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., . . . de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication, 23*(6), 370–388. doi:10.1093/jcmc/zmy020

Braunlich, K., Dienlin, T., Eichenhofer, J., Helm, P., Trepte, S., Grimm, R., . . . Guys, C. (2021). Linking loose ends: An interdisciplinary privacy and communication model. *New Media & Society, 23*(6), 1443–1464. doi:10.1177/1461444820905045

Bucher, T., & Helmond, A. (2017). The affordances of social media platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.), *The SAGE handbook of social media* (pp. 233–253). London, UK: SAGE Publications.

Chen, Z., Jardine, E., Liu, X. F., & Zhu, J. J. H. (2022). Seeking anonymity on the internet: The knowledge accumulation process and global usage of the Tor network. *New Media and Society*. Advance online publication. doi:10.1177/14614448211072201

Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society, 11*(3), 395–416. doi:10.1177/1461444808101618

Costa, E. (2018). Affordances-in-practice: An ethnographic critique of social media logic and context collapse. *New Media & Society, 20*(10), 3641–3656. doi:10.1177/1461444818756290

Couldry, N., & Yu, J. (2018). Deconstructing datafication's brave new world. *New Media & Society, 20*(12), 4473–4491. doi:10.1177/1461444818775968

Davis, J. L., & Graham, T. (2021). Emotional consequences and attention rewards: The social effects of ratings on Reddit. *Information, Communication and Society, 24*(5), 649–666. doi:10.1080/1369118X.2021.1874476

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11*, 763–781.

Denegri-Knott, J., Jenkins, R., & Lindley, S. (2022). Valuing digital possessions: The role of affordances. *Journal of Computer-Mediated Communications, 27*(6), 1–11. doi:10.1093/jcmc/zmac019

Dienlin, T., Masur, P. K., & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society, 25*(5), 1043–1064. doi:10.1177/14614448211016316

Edgett, S. J. (2003). Double-clicking on Fourth Amendment protection: Encryption creates a reasonable expectation of privacy. *Pepperdine Law Review, 30*(2), 339–366. Retrieved from https://digitalcommons.pepperdine.edu/plr/vol30/iss2/4

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication, 22*(1), 35–52. doi:10.1111/jcc4.12180

Faraj, S., & Azad, B. (2012). The materiality of technology: An affordance perspective. In P. M. Leonardi, B. A. Nardi, & J. Kallinikos (Eds.), *Materiality and organizing: Social interaction in a technological world* (pp. 237–258). Oxford, UK: Oxford University Press.

Freedom House. (2022). *Countries and territories*. Retrieved from https://freedomhouse.org/countries/freedom-world/scores

Freeman, J. L., & Neff, G. (2023). The challenge of repurposed technologies for youth: Understanding the unique affordances of digital self-tracking for adolescents. *New Media & Society, 25*(11), 3047–3064. doi:10.1177/14614448211040266

Fu, J. S., & Zhang, R. (2019). NGOs' HIV/AIDS discourse on social media and websites: Technology affordances and strategic communication across media platforms. *International Journal of Communication, 13*, 181–205.

Gallagher, K., Patil, S., & Memon, N. (2017, July 12–14). New me: Understanding expert and non-expert perceptions and usage of the Tor anonymity network. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security* (pp. 385–398). Santa Clara, CA: USENIX Association. Retrieved from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/gallagher

Gliksberg, C. (2017). Decrypting the Fourth Amendment: Applying Fourth Amendment principles to evolving privacy expectations in encryption technologies. *Loyola of Los Angeles Law Review, 50*, 765–792.

Haciyakupoglu, G., & Zhang, W. (2015). Social media and trust during the Gezi protests in Turkey. *Journal of Computer-Mediated Communication, 20*(4), 450–466. doi:10.1111/jcc4.12121

Hart, C., Jin, D. Y., & Feenberg, A. (2014). The insecurity of innovation: A critical analysis of cybersecurity in the United States. *International Journal of Communication, 8*, 2860–2878.

Hosein, G. (2017). Compromising over technology, security, and privacy. *International Journal of Communication, 11*, 902–906.

Jardine, E. (2018). Privacy, censorship, data breaches and internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media & Society, 20*(8), 2824–2843. doi:10.1177/1461444817733134

Johns, A. (2021). 'Are we becoming the kind of nation that just blocks out all criticism?': Negotiating the gap between digital citizenship education and young people's everyday digital citizenship practices in Malaysia. *International Journal of Communication, 15*, 4690–4708.

Kalmus, V., Bolin, G., & Figueiras, R. (2022). Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. *New Media & Society*. Advance online publication. doi:10.1177/14614448221134493

Karahanna, E., Xu, S. X., Xu, Y., & Zhang, N. (2018). The needs-affordances-features perspective for the use of social media. *MIS Quarterly, 43*(3), 737–750. doi:10.25300/MISQ/2018/11492

Karlstrom, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Journal of Social Theory, 15*(1), 23–36. doi:10.1080/1600910X.2013.870083

Kim, D. H., & Ellison, N. B. (2021). From observation on social media to offline political participation: The social media affordances approach. *New Media & Society, 24*(12), 2614–2634. doi:10.1177/1461444821998346

Kini, S., Pathak-Shelat, M., & Jain, V. (2022). Conceptualizing "filter-ing": Affordances, context collapse, and the social self online. *International Journal of Communication, 16*, 1573–1593.

Kozinski, A. (2015). Essay: The two faces of anonymity. *Capital Law Review, 43*(1), 1–17.

Kubitschko, K. (2015). The role of hackers in countering surveillance and promoting democracy. *Media and Communication, 3*(2), 77–87. doi:10.17645/mac.v3i2.281

Landwehr, M., Borning, A., & Wulf, V. (2021). Problems with surveillance capitalism and possible alternatives for IT infrastructure. *Information, Communication and Society, 26*(1), 70–85. doi:10.1080/1369118X.2021.2014548

Lauriano, L. A. (2023). Gay employees on social media: Strategies to portray professionalism. *Journal of Computer-Mediated Communication, 28*(2), 1–14. doi:10.1093/jcmc/zmad001

Lee, F. L. F., Liang, H., Cheng, E. W., Tang, G. K. Y., & Yuen, S. (2022). Affordances, movement dynamics, and a centralized digital communication platform in a networked environment. *Information, Communication, & Society, 25*(12), 1699–1716. doi:10.1080/1369118X.2021.1877772

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication, 11*, 824–842.

Mak, M. K. F., Koo, A. Z.-X., & Rojas, H. (2022). Social media engagement against fear of restrictions and surveillance: The mediating role of privacy management. *New Media & Society*. Advance online publication. doi:10.1177/14614448221077240

Martin, N., Rice, J., & Martin, R. (2016). Expectations of privacy and trust: Examining the views of IT professionals. *Behavior & Information Technology, 35*(6), 500–510. doi:10.1080/0144929X.2015.1066444

Meisner, C., & Ledbetter, A. M. (2020). Participatory branding on social media: The affordances of live streaming for creative labor. *New Media & Society, 24*(5), 1179–1195. doi:10.1177/1461444820972392

Nagy, P., & Neff, G. (2015). Imagined affordance: Reconstructing a keyword for communication theory. *Social Media + Society, 1*(2), 1–9. doi:10.1177/2056305115603385

National Academies of Sciences, Engineering, and Medicine. (2018). *Decrypting the encryption debate: A framework for decision makers*. Retrieved from https://nap.nationalacademies.org/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers

Orman, H. (2015). Why won't Johnny encrypt? *IEEE Internet Computing, 19*(1), 90–94. doi:10.1109/MIC.2015.16

Pagh, J., Skovhoj, F. H. Z., & Lai, S. S. (2022). A good way to talk: A comparative analysis of communication choices in China, Denmark, and the U.S. *Information, Communication, & Society, 25*(15), 2317–2332. doi:10.1080/1369118X.2021.1934067

Pearce, K. E., & Malhotra, P. (2022). Inaccuracies and Izzat: Channel affordances for the consideration of face in misinformation correction. *Journal of Computer-Mediated Communication, 27*(2), 1–19. doi:10.1093/jcmc/zmac004

Pew Research Center. (2018, March 27). *Americans' complicated feelings about social media in an era of privacy concerns*. Retrieved from https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Pew Research Center. (2019, November 15). *Americans and privacy: Concerned, confused, and feeling lack of control over their personal information*. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Rogers, M., & Eden, G. (2017). The Snowden disclosures, technical standards, and the making of surveillance infrastructures. *International Journal of Communication, 11*, 802–823.

Rubel, A., & Biava, R. (2014). A framework for analyzing and comparing privacy states. *Journal of the Association for Information Science and Technology, 65*(12), 2422–2431. doi:10.1002/asi.23138

Sheng, S., Broderick, L., Koranda, C. A., & Hyland, J. J. (2006). *Why Johnny still can't encrypt: Evaluating the usability of e-mail encryption software*. 2006 Symposium on Usable Privacy and Security - Poster Session, 2006, Pittsburgh, PA.

Silverman, J. (2017). Privacy under surveillance capitalism. *Social Research, 84*(1), 147–164.

Singh, S. (1999). *The code book: The evolution of secrecy from Mary Queen of Scots to quantum cryptography*. New York, NY: Anchor.

Siuda, P., Nowak, J., & Gehl, R. W. (2022). Darknet imaginaries in internet memes: The discursive malleability of the cultural status of digital technologies. *Journal of Computer-Mediated Communication, 28*(1), 1–14. doi:10.1093/jcmc/zmac023

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2019). Privacy and the panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society, 21*(3), 602–619. doi:10.1177/146144481880131

Taddicken, M. (2014). The privacy paradox in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*, 248–273. doi:10.1111/jcc4.12052

Tandoc, E. C., Jr., Lou, C., & Min, V. L. H. (2019). Platform-swinging in a poly-social-media context: How and why users navigate multiple social media platforms. *Journal of Computer-Mediated Communication, 24*(1), 21–35. doi:10.1093/jcmc/zmy022

United Nations. (2015, July 1). *Human rights, encryption and anonymity in a digital age*. United Nations Human Rights Office of the High Commissioner. Retrieved from https://www.ohchr.org/en/stories/2015/06/human-rights-encryption-and-anonymity-digital-age

Vagle, J. L. (2015). Furtive encryption: Power, trust, and the Constitutional cost of collective surveillance. *Indiana Law Journal, 90*(1), 101–150.

Vitak, J., Liao, Y., Mols, A., Trottier, D., Zimmer, M., Kumar, P. C., & Pridmore, J. (2023). When do data collection and use become a matter of concern? A cross-cultural comparison of U.S. and Dutch privacy attitudes. *International Journal of Communication, 17*, 471–498.

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Winseck, D. (2002). Illusions of perfect information and fantasies of control in the information society. *New Media & Society, 4*(1), 93–122. doi:10.1177/14614440222226280

Wu, J., & Zappala, D. (2018). When is a tree really a truck? Exploring mental models of encryption. In *Proceedings of the 14th Symposium on Usable Privacy and Security* (pp. 395–409). Baltimore, MD: USENIX.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. doi:10.1057/jit.2015.5