Politics of Compliance: Redefining Perceived Agency in "Wellness"

Morgan Banville, Massachusetts Maritime Academy
Emily Gresbrink, Minnesota State University, Mankato
Elena Kalodner-Martin, The Ohio State University

Our article offers a toolkit for computers and writing scholars and educators to use—for themselves and their students—to address what we refer to as "perceived agency." We find it imperative to create deliverables that can be used as a guide in navigating consent, agency, and privacy. In particular, our article contributes to understanding how perceived agency informs lived experience—and ponders, "in what ways digital technologies mediate, manifest, and manipulate this relationship?" We focus specifically on instances in healthcare, where biometrics in NICU nursing, wearable technologies for diabetes management, and the use of artificial intelligence in crisis communication showcase tensions between perceived agency and embodied, psychological,

The Electronic Frontier Foundation (EFF), a leading nonprofit organization defending civil liberties in the digital world, created a "Surveillance Self-Defense Kit" with the goal of ensuring that technology supports freedom, justice, and innovation for all people of the world (see About EFF). This article extends ideas from the EFF toolkit by offering a guide for computers and writing scholars and educators to use—for themselves and their students—to address what we refer to as "perceived agency." Due to the political upheaval in the United States, we find it imperative to create deliverables that can be used specific to precarious sites such as healthcare to guide in navigating consent, agency, and privacy. In particular, our healthcare toolkit contributes to understanding how perceived agency informs lived experience and questions, "in what ways digital technologies mediate, manifest, and manipulate this relationship?"

We answer this question by troubling agency as a framework to understand not only the range of available actions but the influence that safety, security, and stakes have in contributing to users' perceptions of autonomy. We offer *perceived agency* as a lens for examining how different people assess and act upon their autonomy based on their precarity in different contexts, given their understanding of risk, safety, and consequence. To illustrate such perceptions, we focus specifically on case instances in healthcare, where biometrics in the neonatal intensive care unit (NICU) (Morgan), wearable technologies

DOI: https://doi.org/10.37514/PCW-B.2026.2883.2.04

for diabetes management (Elena), and the use of artificial intelligence (AI) in crisis communication (Emily) showcase tensions between perceived agency and embodied, psychological, and/or material consequences for patients, their families, and the impacts of slow technology (such as referenced in Johnson, Chandler, & Rice, 2024; Ulmer, Sellnow & Seeger, 2022). Slow technology refers to taking the time to see how something works, understanding how it works, applying it, seeing what it is, and finding out the consequences of using it (Hallnäs & Redström, 2001, p. 203). We find that perceived agency and slow technology are two approaches that are necessary to address the implications of health surveillance; for example, employers often incorporate wearable devices within the workplace to increase a more "efficient," "safer," and "healthier" work environment (Zikos & Hodgkins, 2025). Such incorporation, despite the potential for lower insurance premiums or discounts at local fitness centers, creates an *unsafe* work environment due to the increase of surveillance, invasion of health data by corporations and third-parties, and questionable definitions of what is considered "healthy" (see Banville, 2020; Thompson, 2019).

By looking at these three high-risk and high-stakes health settings, we reveal how the 'choices' that are often presented to patients ("users") often obscure the systemic factors that trouble refusal and consent, particularly for those who are already marginalized by nature of their race, class, gender, and more. In doing so, we further complicate what it means to be compliant, and how to subvert the very systems that seek to oppress and control. How can we—as computers and writing scholars and teachers—protect ourselves and the people most likely to *not* have agency or autonomy? Through the use of our toolkit, we advocate for a slow technological approach under the framework of perceived agency as a means to integrate technology in a meaningful way that emphasizes informed consent.

Troubling and Extending Agency

As mentioned in our introduction, while employers assume (and likely believe) that they are contributing to creating a "safe" and "healthy" work environment by implementing new technologies, they are instead subjecting employees to increased surveillance that they are often uninformed about. This opens up space to ask: How is the concept of "health" and "wellness" situated for healthcare professionals, patients, and more?

We want to note that "using technology as a means of improving the quality of life" (Beck, 2018, p. 300) is not a neutral or universally accepted endeavor. The decision to adopt—or refuse—technological interventions is shaped by intersecting factors such as medical authority, social expectations, and

perceived risk, or agency. In the case of biometrics, wearables, and implants, for example, the stakes of compliance are particularly high: Who gets to say no to these technologies, and under what conditions? Who is expected to say yes, and how is their consent shaped by institutional pressures, medical recommendations, or workplace policies? What are the consequences for saying no, especially when these devices are often positioned as being *only* helpful? And, with artificial intelligence (AI) as a prominent player in multiple technology and medical spaces, at what point do we accept or refuse it - and when will that decision be out of our hands (is it already)?

While individuals may appear to have agency in making these decisions, the distinction between having agency and the perception of agency is critical, especially when structural forces like employer mandates, medical guidelines, and financial incentives subtly (or explicitly) coerce compliance. As such, we point out that these questions are not just hypothetical; they have real consequences for patients navigating the fine line between autonomy and adherence. Risk, in this context, is not just about potential device failure or adverse health outcomes but also about the social and professional repercussions of non-compliance. Whether framed as a requirement for insurance coverage, a condition of employment, or a standard of responsible self-management, the expectation to comply with technological interventions has material consequences, reinforcing existing disparities in access, agency, and decision-making power.

Why a Toolkit?

Toolkits offer greater flexibility of use, and for the purposes of this paper, are defined as a grouping of multiple strategies and examples that translate explicit knowledge such as templates, guidelines, case studies, and more to a defined population. Further, toolkits can be used to facilitate change, and can include strategies for guideline implementation, informing policy, and practitioner training (Torrey et al., 2001; Wirtschafter et al., 2011). For example, the Registered Nurses Association of Ontario offers a toolkit on "Best Practice Guidelines" for patient care. Toolkits can be used by computers and writing scholars for promoting best practices as well as providing key roles for instructors in specific fields. For instance, Tham (2018) devised a toolkit that explores seven dimensions of interactivity for wearables and internet of things products and identifies key roles for technical communicators in immersive media design. Such toolkits are essential for providing guidance for implementing strategies and examples into practice.

We find that the questions from the Electronic Frontier Foundation (EFF) Security Plan outlined from 2023 is an effective example of a toolkit. Such

questions, along with resources online, assist readers with outlining ways to protect themselves and those around them, and can be adapted based on location and context:

1. What do I want to protect?
2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?
6. Who are my allies?

The following toolkit offers examples that computers and writing scholars may use in healthcare or crisis communication settings. We believe that these examples are common and demonstrative of the types of plans that instructors, students, practitioners, and patients alike would benefit from having access to.

Creating a Security Plan: Biometrics in the NICU

This section focuses on creating a toolkit for parents and guardians that builds from the 2023 EFF Security Plan questions. In high stress, potentially unanticipated, and emotional situations such as that in a neonatal intensive care unit (NICU), it makes logical sense that a parent's first thought might not be about the tools and technologies that neonatal nurses are using for their newborns. Not only is there a sense of perceived agency with choice—do I *really* have a choice in this situation? —but there are also fraught conditions around refusing biometrics across the globe based on citizenship status, race, class, gender, and sexuality (see Banville, 2023). Biometrics are defined as "any identifier of the body that is collected and used for personal identification (and authentication)" (Banville, 2023, p. 20). Examples range from facial recognition, iris scans, voice recognition, fingerprinting, and more.

Stakeholders, such as nurses, doctors, parents, and guardians, involved in the NICU have a goal of keeping the patient safe. Ensuring both privacy and security for the patient are extensions of some of the more immediate safety concerns. For example, the consequences and implications for those who are undocumented (see Altman, Broder, & D'Avanzo, 2025) refusing biometric usage in a healthcare setting, versus a U.S. citizen, would have varying levels of risk. For those who are undocumented, the refusal of biometric usage would be high risk as they could be labeled as "noncompliant" and thus unwarranted attention might be placed on the individual, potentially leading to denial of care if labeled as a "non-emergency", deportation, and more (for

specific legalese, see D'Avanzo, 2025). On the other hand, if a citizen refuses biometrics, they could also be labeled as non-compliant, but the risk would be significantly lower due to the level of perceived agency (in this particular example). To address such varying levels of risk, it is crucial to create an individualized security plan as modeled by the EFF. In such high stress situations, urgency and fear should not be the motivator to use or opt into biometric usage. Creating a security plan is an example of a toolkit for computers and writing scholars to contribute to documentation design in healthcare settings and implement activities in the college classroom. Furthermore, answering the following questions allows for parents and guardians to prepare their own safety plan for their child, and ultimately, for themselves. The questions can be developed individually or discussed with a trusted provider; it is recommended that such questions are completed prior to labor (this process can be initiated at any reasonable time prior to the day of labor when tensions might be exacerbated). Parents and guardians could consider the security plan as an additional component to the routine checklist that might already be in place; for example, in addition to creating a birth plan, preparing a hospital bag, babyproofing the home, buying a car seat, and much more.

1. *What biometric data do I want to protect? Such biometric data specific to newborns could be fingerprints, handprints/palmprints, ear recognition, and footprints.*

   Parents/guardians typically care about the safety of their child: from mental and physical health, interpersonal relationships, and more, biometric technologies are an extension of the everyday concerns parents may have about their child (see Minkin & Horowitz, 2023). For this question, safety (or protection) could refer to limiting the biometrics that can be collected and ultimately distributed to third-parties such as insurance companies, data brokers, pharmacies, and more. Though such data is subject to compliance measures (depending on the biometric and device), sharing between providers still occurs, security breaches do happen, and unlike a password, your child's biometrics cannot be reset.

2. *Who do I want to protect my biometric data from?*

   Data might be protected from biometric companies, third-parties, law enforcement, and government agencies. Reasons for protection range from privacy invasion, data mining, discrimination, citizenship concerns, inaccuracies and false identification (see Kalisky et al., 2022), and more.

3. *How bad are the consequences if I fail to protect my biometric data or opt out?*

   Potential consequences range depending on positionality: examples include, but are not limited to, data breaches (Hernandez, 2025), misuse (RightPatient, 2023), risk of deportation (DHS, 2025), privacy violations (Brown & Ellena, 2023), insurance premiums increasing (Parson, 2024), and more.

4. *How likely is it that I will need to protect my newborn's biometric data?*

   No matter parent/guardian positionality, it is important to protect both their own biometric data and the data of the patient (child). Consequences will vary, but individuals creating a security plan should review the previous question to determine risk tolerance and allowance (again, this is grounded in positionality).

5. *How much trouble am I willing to go through to try to prevent potential consequences for myself and my child?*

   This question refers to the consequences of sharing biometric data with healthcare institutions, which may have potential legal and social repercussions (see National Research Council US Whither Biometrics Committee, 2010). Further, "trouble" can also mean refusing and/or opting out of biometrics, potentially leading to labels such as "non-compliant" or "suspicious.," which also may lead to "riskier" consequences.

6. *Who are my allies (for supporting my right to opt out of biometric usage)?*

   Answers will vary: who are the people that can be trusted, friends and professionals, alike? Oftentimes, trusted professionals may be doctors with whom you have had an established rapport or history with; generally, healthcare professionals who listen and honor your concerns as well as your own background and expertise specific to your body are those who might be trusted.

One problem with relying on health technologies such as biometrics is that they are fallible, and they have their limits. Welhausen and Bivens (2021) allude to some of these concerns when referencing a case study of two civilian emergency response mHealth apps—Pulse Point and OD Help. Their concerns range from ease of use of these technologies for professionals and

users (usability and medical attention), to the stability of the programs, security or reliability of data and internet connections, and more. mHealth apps are not biometric technologies, yet they harbor biometric identification and information. The mHealth apps can (and are) fallible, which raises concerns about users perceived agency, data protection, and other vulnerabilities. One vulnerability (amongst many others) is that such apps are often assumed to follow HIPAA guidelines but are, in fact, not bound to such guidelines (see Helm & Georgatos, 2014). In the classroom, educators could provide additional examples of vulnerabilities that suggest that newborn biometrics can be altered, distributed, and are inaccurate and biased (see Saggese et al., 2019; Tiwari, 2024).

Opting In and Out for Chronic Care: Wearable Health Technologies for Diabetes Management

Wearable technologies like continuous glucose monitors (CGMs) are life-saving tools for people with diabetes, providing timely alerts, tracking blood glucose trends, and offering data-driven insights for medical decision-making. Yet, for many patients, especially marginalized populations, wearables also introduce tensions surrounding autonomy, consent, and surveillance (Britton & Britton-Colonnese, 2017). This section of our toolkit troubles the dominant narratives surrounding wearables and offers questions for guiding discussions about the unequal stakes and pressures associated with their use, particularly in high-stakes medical settings. Each section offers guiding questions that may open discussions between patients and providers.

1. *Reconsidering Perceived Agency: Who is a "Good Patient"?*

   Patients face not just medical decisions but social and professional pressures that shape their choices. Wearables are often marketed as tools that enhance patient agency, but they can also reinforce the notion of the "good patient" as someone who complies with healthcare recommendations and uses all available technologies, regardless of their concerns. Refusal may carry consequences, including being labeled as "non-compliant" and risking poorer treatment outcomes, such as increased risk of complications, slower recovery times, and even death. Because wearable technologies are only one option among many, questions may trouble the framing of them as the only good or responsible choice.

   - "Are there alternative ways to monitor my condition that don't involve continuous data tracking?"

- "What are the potential trade-offs between using this device and managing my health through other methods?"
- "How can I balance the benefits of wearable data with my concerns about privacy, comfort, and long-term use?"

2. *Navigating Surveillance, Data Collection, and Privacy*

   Concerns about data privacy are echoed by many wearable users, yet most continue using these devices due to the perceived trade-off between health benefits and privacy risks (Banville, 2020). These concerns are often amplified by the lack of digital security, particularly because Health Insurance Portability and Accountability Act (HIPPA) guidelines geared towards patients' data privacy do not extend to devices like the Dexcom or other many Continuous Glucose Monitors (CGMs). This dynamic highlights how consent can be compromised when patients feel pressured to comply, particularly in high-stakes environments like diabetes care. Questions may focus on untangling concerns about data privacy and consent when facing decision-making about wearable health technologies.

   - "Can you explain how this device collects my health data and who might have access to it?"
   - "What are the potential risks to my data privacy, and how are those risks being addressed?"
   - "Who benefits from the data collected by this wearable, and how can I protect my privacy while still managing my health effectively?"

3. *Exploring Informed Consent and Positionality*

   Informed consent is shaped by systemic factors, including racism, sexism, and ableism. Marginalized patients face heightened risks of dismissal, disproportionate financial burdens and insecurities, poorer health outcomes, and pressure to comply with provider recommendations, often under the guise of "shared decision-making."

   Questions can explore how patients from marginalized, underrepresented, or other vulnerable backgrounds can shape informed consent.

   - "Are there alternative options that might better align with my values, and how can I advocate for them in a system that may not prioritize my needs?"

- "Is there someone else I can consult with on using this device?"
- "Are there any risks or biases with using this technology that may disproportionately affect [identity aspect], and how can these be addressed?"

It is important to consider how wearable health technologies do offer invaluable insights for patients, and for many, may be the most accessible option for managing their health. However, they still may introduce questions about the pressures, risks, and implications of opting in *or* out. These guiding questions seek to foster open, patient-centered conversations that consider not only the technical advantages of wearable devices but also the broader implications for informed consent, data privacy, and the equitable treatment of all patients. They may also be adapted for conversations in the classroom, where students can be guided through activities and discussions on the implications of surveillance technologies and data privacy in arenas like healthcare.

Generative AI in Crisis Communications: Mitigating Emergent Situations

When risk evolves into crisis, immediacy and speed become critical variables in response and mitigation. As a particularly fast and accessible tool, generative artificial intelligence (GenAI) tools have emerged as potential first responders. The viability and ethics of GenAI first responders have been explored in some depth (Cheng & Jiang, 2020; Chin et al., 2023;), but a question remains underexplored: can GenAI (or rather, should GenAI) be a replacement for a human respondent in crisis?

Xiao and Yu (2024) asked respondents to evaluate chatbots as first responders in crisis situations. Drawing on Coombs and Holladay's situational crisis communication theory (SCCT), they describe SCCT as an empirical approach to crisis communication and management (Coombs & Holladay, 2002). Importantly, Coombs (2021) notes that SCCT's substructures and crisis typing establish a "base-level," empirical response model focused on instructing and adjusting information. Within that frame, an AI-driven chatbot could, in theory, deliver these empirical, inform-and-instruct messages efficiently (Xiao & Yu, 2024). However, *could* does not mean *should*. Xiao and Yu's study found that chatbots excel in speed, accessibility, and scalability. But the impersonal tone, privacy risks, accuracy, and technical glitches raised significant concerns (2024, pp. 11–12). This suggests that AI may meet the empirical demands of base-level crisis responses, but it struggles to replicate the human judgment, empathy, and contextual awareness necessary in crisis

communication. As such, it is difficult to argue against AI's rapid response as a practical support for crisis management. What this means is that a crisis demands immediacy, and chatbots can meet that need. Overall, Xiao and Yu's study reinforce a critical point: in moments when trust, clarity, and human reassurance matter most, efficiency alone is not enough. Crisis communication still depends on the human capacity to balance speed with sensitivity.

Take for example the integration of GenAI into mental health applications: If a human user finds themselves in a crisis, choosing to hand off empirical decision-making or engaging in conversations with GenAI can be helpful to reduce mental load. For example, the development of culturally-situated chatbots in the southern United States uses GPT-4-to help diverse communities prepare for hurricanes, (Zhao, 2024), similar to a team at UT-Austin's development in 2025 of a multilingual emergency messaging bot (Engel, 2025). On the other hand, handing off empirical decision making to GenAI can edge into potentially dangerous territory. Take into account mental health apps and the surge of GenAI: while some users perceive AI tools positively in mental health contexts (Andrade et al, 2014; Carlbring et al, 2024), other users have experienced detrimental harm from engaging with GenAI during mental health crises, or with chronic mental health conditions; use of some of these have led to violence and death and subsequent lawsuits (Abrams, 2025; The New York Times, 2025).

A key component of this step is perceived agency. While the decision for users to use these apps is key, some of those users may not have known they were engaging with GenAI. Returning to the use-case of mental health applications, the peer-support app TalkLife used AI to alter human-written messages. Koko, another peer-to-peer app, used GPT-3 to construct user-facing messages without informed consent (Neville, 2025). In these situations, perceived agency was not afforded to the users of TalkLife and Koko; they were put into a spot where AI was the norm. In this case, and with others, we recommend that perceived agency should be the norm and fully available in times of crisis so users can openly and transparently choose to engage with GenAI; it must not be veiled or convoluted.

Empirical and automated decision making for the sake of speed and quantity does not necessarily equate to response quality or eliminating stress. We question the idea of prioritizing empirical and automated decision making for the sake of speed and quantity and ask how this impacts quality (while failing to eliminate stress). We also question the perceived agency components of GenAI in times of crisis; the decision to use AI should always fall into the hands of the user - not the creator - and should remain transparent, particularly for tools where precarious conditions (such as mental or physical health and safety) are paramount. While a person may not function as

empirically, quickly, or even correctly as a chatbot or GenAI's large language models (LLM)s, there is the component of empathy, humanism, and personhood which comes with talking *to* a person in emergencies, crisis, or disaster which has an impact (Akerkar & Devavaram, 2015; Gresbrink, 2024; Schoofs, Fannes & Claeys, 2022).

We argue that GenAI tools in high-risk or crisis responses are not always more effective or appropriate. Instead, a more mindful, methodical approach to the crisis is needed, which is modeled from Hallnäs & Redström' slow technology–designing for reflection (2001). Here, we see crisis communication taking up the authors' challenge for technology which "promote(s) moments of reflection and mental rest in a more and more rapidly changing environment" (2001, p. 202). An important clarification must be made; we aren't suggesting crisis responses *be* slow. A crisis always has a sense of urgency and haste that requires immediate attention due to ongoing harm. This process of engaging in slow technology can still be inherently empirical; contingent on the scenario, a disaster or crisis can still call for an empirical response. As technologies change and emerge, we instead call for a mindfulness towards personhood that GenAI cannot yet handle or output. Simply stated: we advocate for thoughtful responses helmed by people, or - if GenAI is unavoidable - guided by mindful exploration and cautionary use and reflection of a person.

With tools for GenAI in crisis a looming potentiality, a list of questions for the toolkit might look like asking if GenAI is the appropriate tool to utilize:

- "Is a generative AI tool the right one to use as a first responder in a crisis scenario?"
- "How many people will be impacted if I use GenAI as a first responder versus if I do this myself, as a person?"
- "Can a GenAI response accurately and appropriately mitigate the most immediate harm in the crisis scenario?"
- "Does a GenAI response further cause harm to people, places, or objects?"
- "Does a GenAI tool's response accurately reflect the human experience and agency of those impacted in a crisis?"

Conclusion: Resisting Hyper-surveillance

Finally, as we explore conversations in perceived agency, consent, and privacy, our toolkit aims to increase access to these critical topics for personal and pedagogical applications. Importantly, it is intended to disperse and increase access to critical information for marginalized or precarious populations; in particular, we write this toolkit for those who are at risk of losing unrestricted access to

timely, accurate, and equity-oriented health information in the aftermath of the 2024 United States presidential election. We believe that autonomy, agency, and consent are critical in both an education and embodied sense, and our toolkit seeks to support those who are most at risk for losing these critical rights.

Further, it is important to note that medical surveillance and biometrics overlap with the current artificial intelligence "hype" that has swept the globe. For example, voice biometrics have been introduced in healthcare offices to help transcribe patient notes, and GenAI tools have been integrated into mental health, such as Headspace's Ebb tool (Headspace). More recently in March 2025, Google claimed that the company would expand its health-related artificial intelligence summaries in search as a way to "improve" their influence in the health sector (Bloomberg, 2025). According to the article, Google also intends to add a separate feature in search called "What People Suggest," which it said aims to provide users with information from people with similar lived medical experiences. As we have discussed, there are risky ethical dimensions associated with the increased usage of AI in healthcare, including the potential surveillant risks and aspects associated with embodied, community care. Furthermore, as surveillance technologies and artificial intelligence move towards a commonplace position, it is essential to know your rights to privacy and autonomy, particularly in the United States. We hope that building a toolkit can be one way to equip stakeholders in resisting hyper-surveillance and the increasing attacks on bodily autonomy and agency.

References

Abrams, Zara. (2025). Using Generic AI chatbots for mental health support: A dangerous trend. https://www.apaservices.org/practice/business/technology/artificial-intelligence-chatbots-therapists#:~:text=APA%20met%20with%20federal%20regulators,director%20of%20health%20care%20innovation

Akerkar, Supriya, & Devavaram, John. (2015). Understanding rights-based approach in disasters: A case for affirming human dignity. In A. E. Collins (Ed.), *Hazards, risks, and disasters in society* (pp. 79-97). Elsevier. https://doi.org/10.1016/B978-0-12-396451-9.00006-8

Altman, Heidi, Broder, Tanya & D'Avanzo, Ben. (2025, August 20). The anti-immigrant policies in Trump's final "big beautiful bill," explained. National Immigration Law Center. https://www.nilc.org/resources/the-anti-immigrant-policies-in-trumps-final-big-beautiful-bill-explained/#restrictions-on-immigrants-health-and-nutrition

Andrade, Laura Helena, Alonso, Jordi, Mneimneh, Zeina, Wells, J. E., Al-Hamzawi, Ali, Borges, Guilherme, Bromet, Evelyn, Bruffaerts, Ronny, de Girolamo, Giovanni, de Graaf, Ron, Florescu, Silvia, Gureje, Oyewusi, Hinkov, Hristo Ruskov, Hu, Chiyi,

Huang, Yueqin, Hwang, Irving, Jin, Robert, Karam, E.G., Kovess Masfety, Vivian, & Levinson, Daphne. (2014). Barriers to mental health treatment: results from the WHO World Mental Health surveys. *Psychological medicine 44(*6), pp. 1303-1317.

Banville, Morgan. (2020). Resisting surveillance: Responding to wearable device privacy policies. In *Proceedings of the 38th ACM International Conference on Design of Communication* (SIGDOC '20). Association for Computing Machinery, New York, NY, USA, Article 29, pp. 1–8. https://doi.org/10.1145/3380851.3416764

Banville, Morgan. (2023). *Am I who I say I am? The illusion of choice: Biometric identification in healthcare.* [Doctoral dissertation, East Carolina University].

Beck, Estee. (2018). Implications of persuasive computer algorithms. In J. Alexander & J. Rhodes (Eds.). *The Routledge handbook of digital writing and rhetoric* (pp. 291-303). Routledge.

Bloomberg. (2025, March 18). *Google to expand AI answers to medical queries in search results.* The Mercury News. https://www.mercurynews.com/2025/03/18/google-to-expand-ai-answers-to-medical-queries-in-search-results/

Britton, Katherine & Britton-Colonnese, Jennifer D. (2017). Privacy and security issues surrounding the protection of data generated by continuous glucose monitors. *Journal of Diabetes Science and Technology, 11*(2), pp. 216-219. https://doi.org/10.1177/1932296816681585

Brown, Jalen, & Ellena, Katherine. (2023, June 6). *Biometric privacy violations: As costs of liability soar, insurance may respond.* Reed Smith. https://www.reedsmith.com/en/perspectives/cyber-insurance-claims/2023/06/biometric-privacy-violations-as-costs-liability-soar-insurance-may-respond

Cheng, Yang, & Jiang, Hua. (2020). AI-Powered mental health chatbots: Examining users' motivations, active communicative action and engagement after mass-shooting disasters. *Journal of Contingencies and Crisis Management*, *28*(3), 339–354. https://doi.org/10.1111/1468-5973.12319

Chin, Hyojin, Lima, Gabriel, Shin, Minji, Zhunis, Assem, Cha, Chiyoung, Choi, Junghoi, & Cha, Meeyoung. (2023). User-chatbot conversations during the COVID-19 pandemic: Study based on topic modeling and sentiment analysis. *Journal of Medical Internet Research*, 25, Article e40922. https://doi.org/10.2196/40922

Coombs, W. Timothy, & Holladay, Sherry J. (2002). Helping crisis managers protect reputational assets initial tests of the situational crisis communication theory. *Management Communication Quarterly*, *16*(2), 165–186. https://doi.org/10.1177/089331802237233

Coombs, W. (2021). *Ongoing crisis communication: Planning, managing, and responding*. Sage Publications.

D'Avanzo, Ben. (2025, October 1). *Fact Checking immigrants, health care, and the 2025 tax and budget law.* National Immigration Law Center. https://www.nilc.org/resources/fact-checking-immigrants-health-care-and-the-2025-tax-and-budget-law/

Department of Homeland Security (DHS). (2025, January 24). *Biometrics.* https://www.dhs.gov/biometrics

Electronic Frontier Foundation (EFF). (2023, October 27). *Your Security Plan. Surveillance Self Defense*. https://ssd.eff.org/module/your-security-plan

Engel, Oliver. (2025) Ai to the Rescue? UT Research Team Develops Multilingual

Emergency Messaging Bot. *Texas Connect,* https://texasconnect.utexas.edu/2025/09/29/ai-to-the-rescue-ut-research-team-develops-multilingual-emergency-messaging-bot/

Gresbrink, Emily. (2024). *A Humanist Approach to Digital Risk Communication: Investigating Graduate Student Responses to COVID-19 E-Mails* [Doctoral dissertation, University of Minnesota].

Hallnäs, Lars, & Redström, Johan. (2001). Slow technology–designing for reflection. *Personal and ubiquitous computing, 5,* 201-212. https://doi.org/10.1007/PL00000019

Headspace. (n.d.). *Meet ebb*. https://tinyurl.com/2bhc4eee

Helm, Anne Marie, & Georgatos, Daniel. (2014). Privacy and mHealth: how mobile health apps fit into a privacy framework not limited to HIPAA. *Syracuse Law Review, 64,* 131-170. https://heinonline.org/HOL/Page?handle=hein.journals/syrlr64&id=139&collection=journals&index=

Hernandez, Joe. (2025, March 24). *23andMe is filing for bankruptcy. Here's what it means for your genetic data.* NPR. https://www.npr.org/2025/03/24/nx-s1-5338622/23andme-bankruptcy-genetic-data-privacy

Johnson, Megan A., Chandler, Eliza, & Rice, Carla. (2024). Resisting normality with cultural accessibility and slow technology. *Leonardo, 57*(2), pp. 215-220. https://doi.org/10.1162/leon_a_02502

Kalisky, Tom, Saggese, Steven, Zhao, Yunting, Johnson, Daniel, Azarova, Maya, Duarte-Vera, Lilia E., Almada-Salazar, Lucila A., Perales-Gonzalez, Daniel, Chacon-Cruz, Enrique, Wang, Jiaxing, Graham, Rishi, Hubenko, Alexandra, Hall, Drew A, & Aronoff-Spencer, Eliah. (2022) Biometric recognition of newborns and young children for vaccinations and health care: a non-randomized prospective clinical trial. *Scientific Reports, 12*(1), pp. 1-8. https://doi.org/10.1038/s41598-022-25986-6

Minkin, Rachel, & Horowitz, Juliana Menasce. (2023, January 24). *Parenting in America Today.* Pew Research Center. https://www.pewresearch.org/social-trends/2023/01/24/parenting-in-america-today/

National Research Council (US) Whither Biometrics Committee. (2010). Cultural, social, and legal considerations. In Joseph N. Pato & Lynette I. Millett (Eds.), *Biometric recognition: Challenges and opportunities.* National Academies Press. https://www.ncbi.nlm.nih.gov/books/NBK219893

Neville, Stephen. (2025). *When help isn't fully human: The problem of generative AI in crisis support*. Just Tech. https://just-tech.ssrc.org/articles/the-problem-of-generative-ai-in-crisis-support/

Parson, Khari. (2024, May 29). *Eyes on the prize: Early developments in the potential use of biometrics in life insurance.* Verisk. https://core.verisk.com/Insights/Emerging-Issues/Articles/2024/May/Week-5/Biometrics-in-Life-Insurance

Registered Nurses' Association Ontario. (n.d.). *Nursing best practice guidelines.* Retrieved April 15, 2025, from http://rnao.ca/bpg

RightPatient. (2023, October 13). *The influence of biometrics on medical data security.* https://www.rightpatient.com/guest-blog-posts/the-influence-of-biometrics-on-medical-data-security/

Saggese, Steven, Zhao, Yunting, Kalisky, Tom, Avery, Courtney, Forster, Deborah, Edith Duarte-Vera, Lilia, Almada-Salazar, Lucila A., Perales-Gonzalez, Daniel, Hubenko, Alexandra, Kleeman, Michael, Chacon-Cruz, Enrique, & Aronoff-Spencer, Eliah. (2019). Biometric recognition of newborns and infants by non-contact fingerprinting: lessons learned. *Gates open research, 3,* 1477. https://doi.org/10.12688/gatesopenres.12914.2

Schoofs, Lieze, Fannes, Gijs, & Claeys, An-Sofie. (2022). Empathy as a main ingredient of impactful crisis communication: The perspectives of crisis communication practitioners. *Public Relations Review. 48*(1). https://doi.org/10.1016/j.pubrev.2022.102150

Tiwari, Shrikant, Singh, Rishav, Singh, Sanjay K., Kilak, Abhishek S., Alkhayyat, Ahmed, & Vidyarthi, Ankit. (2024). Biometrics recognition of newborn: a review. *Multimedia Tools and Applications, 83,* pp. 80129–80159. https://doi.org/10.1007/s11042-024-18508-1

Tham, Jason. (2018). Interactivity in an age of immersive media: Seven dimensions for wearable technology, internet of things, and technical communication. *Technical Communication, 65*(1), pp. 45-65. https://www.stc.org/techcomm/2018/02/02/interactivity-in-an-age-of-immersive-media-seven-dimensions-for-wearable-technology-internet-of-things-and-technical-communication/

The New York Times. (2025). Human therapists prepare for battle against A.I. Pretenders. https://www.nytimes.com/2025/02/24/health/ai-therapists-chatbots.html

Thompson, Dale B. (2019). Balancing the benefits and costs of health data collected by employer-sponsored wellness programs. *Journal of Law, Economics, & Policy, 15,* pp. 141-162. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jecoplcy15&id=166&men_tab=srchresults

Torrey, William C., Drake Robert E., Dixon, Lisa, Burns, Barbara J., Flynn, Laurie, Rush, John A, Clark, Robin E., & Klatzker, Dale. (2001). Implementing evidence-based practices for persons with severe mental illnesses. *Psychiatric Services, 52*(1), pp. 45–50. https://doi.org/10.1176/appi.ps.52.1.45

Ulmer, Robert R., Sellnow, Timothy L., & Seeger, Matthew W. (2022). *Effective crisis communication: Moving from crisis to opportunity.* Sage Publications.

Wirtschafter, David D., Powers, Richard J., Pettit, Janet S., Lee, Henry C., Boscardin, W. John, Subeh, Mohammad Ahmad, & Gould, Jeffrey B. (2011). Nosocomial infection reduction in VLBW infants with a statewide quality-improvement model. *Pediatrics, 127*(3), pp. 419–26, https://doi.org/10.1542/peds.2010-1449

Xiao, Yi, & Yu, Shubin. (2024). Can CHATGPT replace humans in crisis communication? The effects of AI-mediated crisis communication on stakeholder satisfaction and responsibility attribution. *International Journal of Information Management, 80.* https://doi.org/10.1016/j.ijinfomgt.2024.102835

Zhao, Xinyan. (2024). *How generative AI is transforming strategic communication research and empowering the next generation of communication professionals*. UNC Hussman School of Journalism and Media. https://hussman.unc.edu/news/how-generative-ai-is-transforming-strategic-communication-research-and-empowering-the-next-generation-of-communication-professionals

Zikos, Dimitrios, & Hodgkins, Kathleen. (2025). Leveraging the use of wearables in the workplace to improve healthcare providers' well-being. In P. Eappen, N.R. Vajjhala, D. Zikos, K.P. Davidson (Eds.), *Remote Monitoring and Wearable*

Devices in Healthcare. Information Systems Engineering and Management, 63, pp. 147-160. Springer. https://doi.org/10.1007/978-3-031-98897-4_8