2021

The Case of the Nosy Neighbors

Johanna Gunawan

Woodrow Hartzog
Boston University School of Law

MIT Case Studies in Social and Ethical Responsibilities of Computing

The Case of the Nosy Neighbors

Johanna Gunawan[1], Woodrow Hartzog[2]

[1]Khoury College of Computer Sciences, Northeastern University,
[2]School of Law and Khoury College of Computer Sciences, Northeastern University

Published on: Feb 05, 2021

DOI: 10.21428/2c646de5.a4d7f265

ABSTRACT

Inspired by companies like Clearview AI, Nextdoor, and Amazon, this case study asks students to assume the role of a high-ranking ethics-focused employee at a (fictional) neighborhood-focused social media company. It involves challenging ethical questions around how social media services and surveillance tools are built and used, and the complicated relationship between companies, their users, and law enforcement authorities. Students should pay particular attention to the values implicated by certain design decisions, and the competing incentives for corporations that might complicate the picture for ethical decision making.

Johanna Gunawan

Khoury College of Computer Sciences, Northeastern University

Woodrow Hartzog

School of Law and Khoury College of Computer Sciences, Northeastern University

Keywords: *user data privacy, technology in norm enforcement, facial recognition, mass surveillance, mass scraping of public data*

Author Disclosure(s): None to report.

Background Information

Congratulations! You've just been hired as the chief ethicist for NIMBY, a residential neighborhood social media app built to connect people living in geographic proximity to each other. Your job as chief ethicist is to advise NIMBY's corporate leadership, in particular the technical teams under the chief technology officer (CTO) and chief information security officer (CISO), as they build out a service that remains relevant and useful in this new era.[1] The list of responsibilities included in the job posting were:

- Analyze and critique project proposals for ethical gaps in technologies
- Collaborate with and advise technical and business development teams on feature requirements and security

- Design solutions that help NIMBY achieve business goals with minimal consequences to privacy, civil rights, and marginalized populations
- Identify and describe the short- and long-term consequences of technical or business suggestions
- Consider and evaluate potentially conflicting values or goals-specific decisions and projects as a whole
- Suggest technical or business solutions or additional provisions in the interest of ethical decision making
- Utilize any existing technical, business, legal, or other background expertise to provide suggestions and critique on project proposals

After accepting and signing NIMBY's offer, you hope for smooth entry into the role.

Crisis Strikes

Unfortunately, the week before your first day is rife with turmoil as a global public health concern arises, forcing governments to demand public compliance with new rules requiring home isolation and self-quarantining. Humanity as a whole benefits when everyone complies, but the public health rules constrict individual freedoms and daily living. Most people comply and stay inside, but some still stubbornly go about their day as if nothing were wrong. Governments around the world are stretched thin and unable to enforce their own stay-at-home orders with their existing police. The government of Northernstate recently approached NIMBY, hoping to set up a partnership that will leverage your company's technology to better ensure enforcement of the stay-at-home rules. They believe that working with grassroots, neighborhood watch–like social structures can help them crack down on violations and issue fines.

NIMBY's headquarters are situated within Northernstate's capitol. This provides NIMBY a slight advantage when collaborating with policymakers, as compared to competing services that operate out of distant technology hubs. That being said, NIMBY's geographic proximity and the capitol's social circles mean that NIMBY is subject to closer scrutiny with regard to NIMBY's cutting-edge technologies, especially when technological developments clash with legislators' concerns. NIMBY also regularly lobbies governments like other tech companies do, for better or for worse.

As you settle into your new office on your first day, you sink into your ergonomic chair and begin thumbing through the welcome packet on your desk.

Welcome to NIMBY!

We are so happy you joined our team of forward-minded individuals. We look forward to working with you and making the world, and your neighborhood, a safer place for all.

A Bit About Us

Our company mission serves dual purposes: connecting neighbors to build their social capital with each other while helping communities stay safe and secure. Users have called us their favorite way to get to know the people around them, as well as "the best tool a Neighborhood Watch could ask for."

The NIMBY platform currently offers the following features for our users:

- Forum-style board for people residing in the same area to interact and share media
- Ability to upload posts and photos of suspicious happenings in the neighborhood, or community events (e.g. sharing photos from garage sales and block picnics)
- Tagging abilities—users can tag their own or their neighbors' images with other users

We collect and store this data securely, and use this information to improve our services, suggest potentially matching tags to users, and make the customer experience in NIMBY more fluid.

We're Growing!

Recently, we acquired a promising start-up called "I See You," which claimed to have the best facial recognition software and database in the world. The start-up product is currently in beta, but with the purchase, we here at NIMBY have full rights to experiment with the service. We have taken ownership of I See You's servers, and our technical teams have completed the necessary steps to secure I See You's integration and migration into NIMBY.

We're also currently in talks with other companies, to help expand our abilities and deliver quality services to our customers.

Who You're Working With

NIMBY's technical team is well-versed in basic cybersecurity priorities like confidentiality, integrity, and availability. Our engineers practice security principles throughout each step of the development lifecycle, diligently document their work, and regularly audit our infrastructure to conform to industry standards from the National Institute of Standards and Technology (NIST), and the International Organization for Standardization (ISO).

Over the coming weeks, you'll meet with integral collaborators from the C-suite, our technical teams, and our project management rock stars.

Let's Get You Started

Please review the attached roadmap and project documents as you familiarize yourself in your new role. We're so excited to hear your ideas and start implementing them. Let's make our neighborhoods a

safer place!

Your First-Year Roadmap

We're thrilled to have you on board as our chief ethicist. It's a new role, but one that we consider necessary to help NIMBY grow as a company while staying competitive, relevant, and compliant.

Rising to New Challenges

A lot has changed in the weeks of preparation leading up to your onboarding. The government of Northernstate has run into two major problems in trying to enforce its stay-at-home order. First, the local government doesn't have enough eyes on the ground. It can monitor public squares and high traffic areas easily enough. But it doesn't really know what's happening in more residential areas. Second, even when it does notice people who are violating the stay-at-home order, it often cannot identify the violator. Northernstate hopes NIMBY will not only help crowd-source surveillance through the app's users (and their data), but also aid users in identifying violators through the use of its new startup's highly touted facial recognition tools.

Three Main Priorities

We believe NIMBY is uniquely positioned to help alleviate some of the Northernstate government's problems by implementing new features. As such, our technical and corporate development teams require your advice on three major projects on our twelve-month roadmap:

1. Build a bigger, better faceprint data set
2. Facilitate a partnership with Sahara, a cloud computing provider, and their new camera-enabled doorbell product
3. Leverage the NIMBY user-base to create value-adds for our government clients

For the Next Team Meeting

While you settle in, take a look at the materials our project management team put together and start thinking about what you'll recommend. We plan to complete each project in succession, so make sure that your ideas for Projects "Stronger Together" (Project 2) and "Helping Hands" (Project 3) build upon previous solutions you design, beginning with Project "Growth Hack" (Project 1).

Every solution you design should include proposed features that satisfy the minimum requirements and goals of each project. Make sure to cover high-level technical and ethical descriptions, then be able to explain why you came to those decisions. Include any diagrams, mock-ups, or visual elements that would help you pitch your constraints to the rest of our C-suite.

Project Documents

1. Project Growth Hack: Build a Better Faceprint Data Set

NIMBY users previously had to rely on neighbors to identify each other or suspicious individuals in photographs or video, which was a manual effort and time-delayed based on neighbors' activity in-app or logins. Users have complained about this, especially in time-sensitive situations like potential burglary.

NIMBY has a fairly quick algorithm for identifying people who have already been tagged multiple times within NIMBY's database. The problem? The faceprint database is too small—it's limited only to data collected within a certain radius to a user's neighborhood and how many peers are using NIMBY. In denser neighborhoods, like in big cities, NIMBY is only as useful as the rate of NIMBY membership in the community. Our faceprint database cannot accurately identify outsiders or visitors in a neighborhood if visitors come from outside the neighborhood's geographic radius. We know that NIMBY is a useful tool, but we need more data to truly be effective.

One of our CTO's brightest engineers suggests scraping public profiles of people thought to be living in certain locales, like photographs from Twitter or Facebook for people who have their location filled out. This was the tactic deployed by Clearview AI,[2] which boasted of having one of the largest faceprint databases in the world. Clearview AI defended its actions by arguing that public photos are fair game. This engineer also argues that scraping is fairly simple and would not require too many hours of the development teams' time to implement. This strategy would free up space for other priorities and cost NIMBY very little in operational costs. The rest of the C-suite seems receptive to this idea and enthusiastic about the potential benefits to the company and bottom line.

Faceprints created by the NIMBY user-base are not enough to power a facial recognition system that can identify suspicious parties beyond a critical mass, as some may come from neighboring cities to avoid immediate detection. Your CEO is pushing an auto-tag feature for quick release — especially because other neighborhood applications seem to be developing similar features.

Right now, NIMBY's database is especially underequipped to identify violators of the stay-at-home policy.

Implementing this within two fiscal quarters would:

- Allow the new safety feature to be released quickly, which would give NIMBY a competitive advantage over other services
- Increase sustained usership within the NIMBY Network, allowing NIMBY to grow with less threat of new users quickly switching to other platforms

- Lead to mergers with other companies or buyouts of other startups
- Open up new opportunities for government collaboration and services exchange; for example, a mutually beneficial arrangement to enable NIMBY to assimilate mugshots into the database in exchange for providing law enforcement facial recognition services
- Improve public health outcomes and neighborhood safety from criminal threats

Not collecting this data might:

- Lead users to choose other platforms
- Allow users' current disgruntlement with "annoying" or "burdensome" features to fester
- Lead to less engagement with the platform, resulting in less granular data for targeted advertising, a key component of NIMBY's business model.

Consider the ethics of photo-scraping and auto-tagging and design a solution for moving forward on this project. Your suggestions must be compatible with these project goals:

- Improve the existing tagging feature in NIMBY, in particular increasing automated methods
- Alleviate user complaints with the manual nature of the feature
- Partially contribute to improved compliance of Northernstate's stay-at-home orders

2. Project Stronger Together: Hardware Partnerships and Community Involvement

Digital infrastructure juggernaut Sahara noticed NIMBY's community safety successes earlier this year and approached our business development teams to form a mutually beneficial partnership. They're looking to distribute their new product on the market, a digital doorbell with camera features called "Sahara's Bell."

Representatives from Sahara contacted NIMBY and proposed a special and quite heavy discount on the hardware for NIMBY users, in order to partner with NIMBY and share the database of recorded video taken from the device. Sahara thinks their IoT doorbell will be more attractive to users if it has NIMBY app capabilities. Sahara also offered access to their data management and cloud computing tools, which could help NIMBY grow exponentially on top of the exposure that a partnership with Sahara could provide. Images and video from the doorbells would be kept in Sahara's databases, with authorized access for approved members of NIMBY's technical and ethical teams.

Implementing this within two fiscal quarters could:

- Garner considerable press for NIMBY, helping it compete in the app market
- Establish a closer partnership with Sahara for future possible projects

- Build a stronger network effect, helping ensure that NIMBY users have another reason not to switch services
- Lead to future, highly lucrative and competitive government contracts for data services
- Potentially aid police in difficult investigations or mass safety measures

Not implementing this feature might:

- Lead to Sahara taking their business elsewhere
- Make NIMBY fall behind the competition and lose out on revenue, user base, and partnerships

Consider the ethics of NIMBY's partnership with Sahara for their IoT doorbell, and again provide your suggestions for moving forward. Your solution must meet the following project goal:

- Increase NIMBY's community data set, whether that be through better user-provided tags, photographs, videos, location/motion data, and so on.

3. Project Helping Hands: Mobilize Users to Catch Violators

Your work on the previous projects will help reduce user complaints about previously "clunky" features of the NIMBY app. Some initial models run by the research department show that NIMBY's facial recognition tools and IoT doorbells can contribute to improved rates of compliance with the stay-at-home order.

Moreover, NIMBY's data shows that users are increasingly frustrated with others in their communities who still evade the stay-at-home rules.

Consultants put forth the idea that mobilizing users—the bread and butter of NIMBY—could be the most effective way to leverage NIMBY's network against noncompliant individuals. NIMBY users could be nudged and supported in identifying and reporting their neighbors for violating stay-at-home orders. Engineering managers suggest a reporting feature for NIMBY's app that would enable users to leverage NIMBY's ability to automatically identify users via photographs or recorded footage with the facial recognition algorithm. This reporting feature would automatically detect and flag anyone in the image who is out and about after predetermined local curfew hours or socializing without a facemask in violation of public health rules. All users would have to do is enable the "report wrongdoers" feature in the NIMBY app with a simple toggle button, and everything captured and flagged would be queued up for reporting to law enforcement authorities.

To avoid false positives, the team suggests a quick prompt for user verification to review what they recorded, which after approval will then automatically provide law enforcement screenshots or videos, timestamps, the names of the reporter and violator, and other useful information. Your development

teams think it's reasonable to implement these quickly, as it would function off of existing architecture with relative ease. They even propose a way to keep the identity of the reporting NIMBY user anonymous, to encourage more tips and information to law enforcement. If these deidentification features were implemented, NIMBY users could report potential illegal activity to police without worrying about getting further involved with the violation.

Implementing this within a fiscal quarter could:

- Potentially "flatten the curve" by identifying individuals violating stay-at-home and increase the number of people being tested
- Encourage users to be more active on the app, improving granular data for ad targeting
- Give users a sense of empowerment and community responsibility

Not implementing this feature might:

- Fail to help mitigate a national crisis
- Lead media outlets to find NIMBY's lack of action part of the issue, thus creating bad press
- Lose first-mover's advantage on the new market for reporting apps

Consider the ethics of NIMBY's proposed "reporting feature" and design a solution that achieves the following goal:

- Motivate NIMBY users to participate in community-based health initiatives and comply (or help others comply) with public health standards

Glossary

Opt-in: A process for agreeing to something, which requires affirmative consent. Example: "Yes, sign me up for monthly emails."

Opt-out: A process for withdrawing typically assumed consent or agreement. Example: "Unsubscribe me from monthly emails," assuming that the person was automatically registered for said emails.

CEO: Chief executive 0fficer. The highest executive-level leader at a company, who typically communicates with shareholders and the board of directors (external corporate leadership), and acts as the face of the company.

CTO: Chief technical officer. An executive-level leader at a company who typically oversees the engineering and technical teams.

CISO/CSO: Chief information security officer, or chief security officer. An executive-level leader at a company who typically oversees data security and protections, which span both internal and external

technical security.

C-Suite: The group of executive leaders at a company, who typically hold titles beginning with "C" (CEO, CTO, CISO, etc.).

Scraping: The collection of information online en masse, using automated tools. Information collected can include text, photos, and other media.

False positives: Results for tests (typically for matching or identifying things) that falsely claim the item in question is what the test seeks. Example: an image-recognition tool that incorrectly identifies a stick as a pencil.

False negatives: Results for tests that incorrectly claim an item in question as something other than the label a test seeks. Example: an image-recognition tool that incorrectly says a pencil is not a pencil.

Discussion Questions

Scraping

Some information online is publicly available—for example, many social media platforms make user icons public by default, even if the user's account is private and only visible to approved followers. Technological advances in computing power make the mass collection of this data not only possible, but relatively effortless.

Is publicly available data, including photographs and location information, "fair game" for mass collection? Why or why not?

Privacy in Public

Privacy has long been debated with regard to the physical location of where a person might be—for example, expectations of privacy are different in your home's bathroom versus the food court of a shopping mall. CCTV cameras are not new and have been in use for many years in public spaces for a variety of security reasons.

Do the Sahara's Bell cameras meaningfully differ from CCTVs? Do neighbors have a reasonable expectation of privacy when, say, picking up their mail at the end of their driveway if the house across the street has a Sahara's Bell installed?

How public (or private) are residential sidewalks or house-fronts? Is there a tangible line that can be drawn to separate public residential areas from private residential spaces—in sparse suburban settings or high-density apartment buildings?

Surveillance as Norm Enforcement

Combined pressures of global health crises and community security add a sense of urgency to the development of any features meant to assist with these issues. The role of government is to assist civilians and provide guidelines for the public that promote health and safety. Companies like NIMBY attempt to provide alternative or supplementary solutions to improve users' lives.

Consider your proposal for Project Helping Hands (Project 3). What benefits do each party receive between the government, NIMBY (including shareholders), and civilians? Who benefits most/whose needs are addressed most?

Now imagine your solution is implemented as-is, with no pushback from any stakeholders. What ways might any involved party misuse or abuse the feature you proposed?

Cultural Norms on Privacy and Surveillance

Northernstate has its own unique perspectives toward civilian independence, privacy, and group surveillance.

How might your suggestions change if NIMBY were located in different countries? What if NIMBY were an app developed for a country with an existing, robust digital surveillance culture? Conversely, what if NIMBY were built in a region with stricter definitions of personal privacy or firmer commitments to privacy and data protection as fundamental human rights?

Competing Pressures in Technological Development

Technology moves quickly, but certain world events can restrict development timelines and force teams to omit research or features in favor of releasing some minimum viable product on time.

As you designed your solutions, what pressures did you feel while trying to complete your goals?

Did you feel you had enough information or time to do your job and conduct a proper analysis of each project's ethical implications and risks? If not, what additional information do you think you would have needed?

Additional Resources and Readings

Clearview AI

Heilweil, Rebecca. "The World's Scariest Facial Recognition App Company Keeps Lying." *Vox, February 11, 2020*. https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement.

Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *New York Times, January 18, 2020*. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Lipton, Beryl. "Records on Clearview AI Reveal New Info on Police Use." *MUCKROCK, January 18, 2020*. https://www.muckrock.com/news/archives/2020/jan/18/clearview-ai-facial-recogniton-records/.

Mac, Ryan, Caroline Haskins, and Logan McDonald. "Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA." *BuzzFeed News, February 27, 2020*. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

IoT Security/Amazon Ring Doorbells

Cericola, Rachel. "Ring Neighbors Is the Best and Worst Neighborhood Watch App." *Wirecutter: Reviews for the Real World*, October 15, 2020. https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/.

Fernandes, Earlence, Amir Rahmati, and Nick Feamster. "New Problems and Solutions in IoT Security and Privacy." *Preprint, submitted October 8, 2019*. http://arxiv.org/abs/1910.03686.

Fussell, Sidney. "Amazon Ring Will Survive the Anti-Surveillance Backlash." *Atlantic, June 2019*. https://www.theatlantic.com/technology/archive/2019/06/police-offer-amazon-ring-free-exchange-access/592243/.

Guariglia, Matthew. "Five Concerns about Amazon Ring's Deals with Police." *Electronic Frontier Foundation, August 2019*. https://www.eff.org/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police.

The Legality of Scraping

Bonifacic, Igor. "Facebook and Venmo Demand Clearview AI Stops Scraping Their Data." *Engadget, February 2, 2020*. https://www.engadget.com/2020-02-06-facebook-venmo-cease-and-desist-clearview-ai.html.

Porter, Jon. "Facebook and LinkedIn Are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech." *Verge, February 6, 2020*. https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube.

Privacy, Obscurity, and Anonymity

File, Patrick C. "A History of Practical Obscurity: Clarifying and Contemplating the Twentieth Century Roots of a Digital Age Concept of Privacy." *University of Baltimore Journal of Media Law & Ethics* 6, nos. 1–

2 (2017): 4–21. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ubjmleth6&section=5.

Hartzog, Woodrow. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA: Harvard University Press, 2018. https://www.hup.harvard.edu/catalog.php?isbn=9780674976009.

Hartzog, Woodrow, and Evan Selinger. "Big Data in Small Hands." *Stanford Law Review 66 (2013)*. https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-in-small-hands/.

Hartzog, Woodrow, and Evan Selinger. *Surveillance as Loss of Obscurity*. Rochester, NY: Social Science Research Network. SSRN Scholarly Paper, January 7, 2016. https://papers.ssrn.com/abstract=2711816.

Peppet, Scott R. "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future." *Northwestern University Law Review* 105, no. 3 (2011): 1153–1203. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1157&context=nulr.

Appendix: Instructor Guidelines

How to Use the Case Study

This case study is intended for high levels of instructor customization and is purposely open-ended. At a minimum we suggest the following:

1. Read through the student materials and consider:
    1. Your desired duration for this project
    2. The type of deliverables you would like students to provide
    3. The scope and level of detail you aim to explore with the deliverables
    4. Whether the students will work in groups or independently
    5. Your primary focus for student discussion: the technology? ethical questions? the process of designing a solution?
2. Prepare your adjustments or any supplements to the student materials
3. Provide students the materials included above, as well as the glossary and reference list as additional resources
4. Use the Follow-up Discussion Questions to guide your own instruction, or provide these to students after case study completion

Student Deliverables and Outcomes

Students should work to deliver solutions to each of the three NIMBY projects. We left the ultimate form of the student deliverable open-ended to adjust for different disciplines or student groups participating in the case study. Instructors are free to choose whatever deliverable they would like to

receive. Instructors can elect to have deliverables be provided within the roleplay framework, or outside of it. A few example deliverables could be:

- A formal project proposal document, detailing the devised solution from a business perspective
- A presentation
- A software prototype or mock-up
- A research paper, memo, or report walking through possible solutions and outlining pros and cons
- A list of follow-up questions, outlining additional details or information students think are necessary to making a sound solution
- A list of imagined outcomes, using student-provided what-if's (for example, students may provide multiple solutions dependent on external events they identify as likely)

Any deliverable should meet the minimum requirements outlined for each project, as well as:

- Convey an understanding of competing interests at play and values served or neglected by specific decisions
- Demonstrate potential costs or consequences/pros/cons of the proposed solution
- Identify impact of the solution on stakeholders/NIMBY/consumers/society

… and any additional requirements you as an instructor would like to see from your students.

However you choose to implement the study, students should broadly think about these issues surrounding the social and ethical responsibilities of computing: facial recognition, technology in norm enforcement, technology as surveillance, and mass scraping of public data. This case study is also designed to encourage students' development of these skills: ethical and critical thinking, prioritization, balancing internal and external corporate pressures, informed and reasoned decision making, project management and design.

Adapting the Case Study

This case study is designed to be modular and flexible, for use in group projects or independent work, and as simulated practicum or thought exercise. You can elect to use all three projects, or just the first project or the first two. Each project is designed to build upon previous projects and escalate tensions within NIMBY between ethical considerations and other incentives.

We envision the case study being implemented in the following examples, but the sky's the limit when encouraging students to ponder tech ethics:

- A three-week group project module with robust deliverables, with one NIMBY project tackled per week
- A one-week, in-class group activity with smaller deliverables

- A single in-class discussion using only the goals outlined in the first-year roadmap, ideally to take place after previous instruction on ethics in tech
- A three-week online or in-person discussion activity, with individuals or groups assigned chief ethicist or ombudsperson roles, in which students in the chief ethicist roles present or write out a solution and other students defend or challenge the solution
- Splitting the projects between student groups

The project goal statement in each project document offers minimum, open-ended requirements for students to deliver on—instructors should further outline the format for student submissions. However, instructors from different fields may have other considerations for students to think through, like technical requirements or policy requirements. Additional parameters can be added to suit different disciplines' needs beyond the existing material—for example, computer science courses could require more detailed technical explanations for each solution, perhaps describing real-world implementations for the students' suggestions.

You can also expand or change the case study to include other roles briefly mentioned in the student materials, like the CEO, CTO, and so on. Doing so will expand students' understanding of how every employee partakes in ethical decision making. (The framework of this case study aims to first outline how someone explicitly charged with this task might need to operate against competing priorities, but we warmly encourage expanded adaptation.) These materials are meant to be a springboard to guide students' critical thinking and discussions, and you can adapt, expand, and contract the items included in this case study however you see fit.

Footnotes

1. See Glossary for additional information about terms such as "CTO," "CISO," and so on. ↩

2. *Clearview AI is a real-world company, which became controversial in 2020 for scraping public images online and assembling these into a sizeable database. See "Additional Resources and Readings."* ↩