From Individual Consent to Collective Refusal: Changing attitudes toward (mis)use of personal data

Big tech companies have been found to misuse personal data, often collected without consent. What can the public do to change unjust collection and use of their personal data, and what role can computer scientists play in these efforts?

By Jonathan Zong

DOI: 10.1145/3433140

In January 2019 IBM published roughly a million photos of unsuspecting people with the goal of improving facial recognition software, many of those people were surprised and upset. IBM promised a chance to opt out, but many thought that wasn't enough. After over a year of advocacy, research, tech workers organizing, and class action lawsuits challenging IBM and other tech firms on the risks and errors of facial recognition, IBM announced in June that it would no longer offer, develop, or research the technology.

The movement against facial recognition is just one of several collective actions that have challenged the collection and use of personal data. As companies and researchers build and market technologies for mass surveillance, incarceration, and deportation to police agencies, including U.S. Immigration and Customs Enforcement (ICE), the public has expressed concern for the risks of mass data collection.

At one time, computer scientists and regulators thought of data collection as an individual privacy rights issue. In this framing, the risks associated with data collection come from what data collectors know about each individual person. These risks are managed through a series of individual choices to share or hide data. However, no individual decision about a single piece of data can meaningfully change broader surveillance systems involving multiple commercial, government, and academic actors.

A previous generation of software engineers and computer scientists told people to either consent or opt out of services that collect data [1]. Recent approaches to tech industry regulation—such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)—have required tech companies to make more individual consent choices available to their customers. But for

many people, managing specific pieces of data is no longer enough; they are now organizing themselves in order to change what data collection systems do and how they work.

To understand this growing approach known as "collective refusal," we need to see the limitations of individual consent more clearly.

HOW INDIVIDUAL CONSENT DIVIDES AND CONQUERS

Although the idea of consent was developed to protect individual rights from powerful groups, it splits decisions about data privacy into an impossible task that no one can reasonably be expected to manage [2]. Few people have the time and capacity to continually gather up-to-date information on how their data is collected, used, and transferred between different entities. In spite of this, corporate policies, academic research, and government regulation shift responsibility away from powerful data collectors and onto individual people when it comes to managing consent for the collection of personal data [3].

HOW INDIVIDUAL CONSENT DOESN'T PROTECT AUTONOMY

Some critics of individual consent argue what often passes for consent in practice doesn't always afford the protections to individual autonomy that it promises in theory.

With individual consent, individuals are expected to make informed, personal decisions about their own welfare. However, a single consent decision often affects multiple people. For example, Dr. Amy Hasinoff, who studies how intimate imagery circulates, has pointed out photographs often include more than one person. The person who takes the photo might not appear in the image, and the person uploading a photo to an online service might be another person altogether. When multiple people have legitimate interests in the circulation of data, no individual-choice consent decision can protect everyone's interests—especially if they don't all agree.

Furthermore, many uses of data also affect people across society, not only those directly involved in data collection. A single photo on its own has limited uses. In contrast, large photographic datasets can be used by facial recognition algorithms and incorporated into abusive policing and immigration systems. Because individual consent is only meant to help people

Image by Piscine26 / Shutterstock.com

manage risks to themselves, it cannot prevent risks to society at large.

HOW POWERFUL ACTORS ABUSE INDIVIDUAL CONSENT

Individual consent is supposed to protect people from abuses of power, but that's not possible when data collectors can use their power to influence consent decisions. Data collection often happens within an unequal power relationship in which the data collector is in a position of authority. This unequal power relation is reinforced by information asymmetry between the data collector and participants, who are rarely aware of how their data is used.

Decisions to collect personal data rarely involve the people whose data is sought. For instance, airlines who are replacing boarding passes with facial recognition scanners did not seek the input of international passengers before implementing these systems. When the scanners appeared in airports, they took many people by surprise—but few passengers are empowered to rock the boat in the security line. The choice to say yes or no to individual cases of data collection doesn't give power to change broader agendas of personal data use.

HOW INDIVIDUAL CONSENT IS USELESS OVER TIME

Individual consent assumes people can make a one-time decision at the point of data collection that forms an agreement about how the data will be used. Yet online data collection happens on an ongoing basis. In addition, new developments in data collection, use, and disclosure are continuously being invented.

Consider the case of IBM's Diversity in Faces dataset, which investigative journalists pointed out was collected without consent using images from Flickr, a photo site started in 2004. Even if people had consented to the use of their images, they couldn't have imagined how their data would be passed around and re-used. Over the next 15 years, photos on Flickr were acquired by a sequence of four companies and hundreds of academic research teams, even as photos from other sites were also added to the archive. At one end of this chain, IBM researchers downloaded a copy of the dataset from Yahoo in 2019 and modified it to create the Diversity in Faces dataset, which resulted in multiple class-action lawsuits.

No one-time decision could possibly manage this complex web. Even worse, it's almost impossible to track down who has a copy of one's data. Especially when companies and individuals download the data, make derivatives, and publish new datasets.

COLLECTIVE REFUSAL: MOVING BEYOND INDIVIDUAL CONSENT

If individual consent can't protect people, what else can people who aren't computer scientists or legal experts do about the ongoing collection and misuse of their personal data, in situations where they lack power?

Researchers have recently described refusal as a "necessary corollary" to consent. For Ruha Benjamin, refusal is a form of agency that involves "refusing the terms set by those who exercise authority in a given context" and which "may also extend beyond individual modes of opting out to collective forms of conscientious objection" [3].

When people included in the IBM dataset organize class-action lawsuits to challenge IBM's use of their personal data, they are going beyond the constraints of individual consent to challenge the underlying system. That is a case of collective refusal.

Refusal is broader than merely saying "no" to individual consent. Instead, it's a way to think about practical actions that people employ to reject data collection and misuse. While approaches to refusal vary in important ways, successful collective refusal questions the terms created by data collectors and challenges the structures that they use to divide and conquer (such as individual consent).

Because everybody is different, no one-size-fits-all approach will be able to address fundamental issues with individual privacy management.

WHAT CAN COLLECTIVE REFUSAL LOOK LIKE?

Collective action can help people address the autonomy problem, manage data over time, and replace individual disempowerment with collective power.

In many high profile instances of collective refusal, successful change is driven by multiple approaches to refusal acting in concert from many different groups within an ecosystem. At its best, collective refusal is led by members of communities most affected by data (mis)use, and aided by other forms of refusal driven by tech workers and researchers. For instance, recent action to refuse the government's use of face surveillance technology in policing has involved steps taken by people affected by facial recognition. The people included in IBM's dataset refused to follow the limited opt-out process offered by the company, and instead filed class-action lawsuits against IBM. Simultaneously, members of groups like the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation (EFF) pressed local governments to pass legislation banning the use of face surveillance. Advocacy groups, like the Stop LAPD Spying Coalition, also sued police to release information about surveillance programs. These were actions that any member of the public could participate in.

Alongside these actions, collective efforts by tech workers within large companies have worked toward building power to change unethical business practices. A letter signed by more than 450 Amazon employees called for the company to stop selling facial recognition to police departments. Similarly, more than 200 employees at Palantir have urged the company to stop providing deportation and tracking software to ICE. As part of the No Tech for ICE campaign, [1] students at universities, such as MIT, Stanford, and Berkeley, have pledged not to work for Palantir while it provides these ser-

[1] https://notechforce.com/

vices. Researchers are also playing an important role in advancing change. Scholars like Joy Buolamwini [4] and Timnit Gebru have educated practitioners about racism in technology through their research. Buolamwini has advocated and testified before Congress, while also contributing to public conversations through poetry and a widely-screened documentary film. Many computer scientists have also joined collective efforts to caution against the publication of flawed science used to legitimize surveillance practices in policing.

In addition to activism and efforts that make use of the legal system, collective refusal by members of the public can start with small actions that grow in power as more people join. For example, a person browsing the internet using Tor software has their traffic anonymized by the network. However, their computer is also participating in the network and helping secure other people's data. People have used collective power to compete with or influence large companies who have neglected to meet their needs. Grassroots internet cooperatives have developed infrastructure to share community-managed internet access without the involvement of large telecom companies in order to make up for the lack of adequate service in their area. Reddit participants have protested company decisions by shutting down online communities, highlighting their importance to the platform.

UNDERSTANDING COLLECTIVE REFUSAL AS COMPUTER SCIENTISTS

As the public is starting to take up collective refusal as a way of reimagining power and affecting change, how should we computer scientists—who design and build tech products or research new ways of using personal data—understand instances of collective refusal? A natural inclination is to wonder whether we can design better individual consent. After all, current individual consent procedures aren't perfect, and offering more choice doesn't sound like a bad thing. As researchers have shown, the difficulty of individual privacy management is often exacerbated by "dark patterns"—user experiences designed to mislead people into handing over their data. Designers and engineers can try to implement better user experiences for managing privacy, but face difficult decisions along the way. For instance, how granular should privacy options be? Unpack every instance of data collection into its own option, and people become overwhelmed with decisions. Bundle options together, and people might face all-or-nothing decisions between accepting data collection or leaving services altogether. Because everybody is different, no one-size-fits-all approach will be able to address fundamental issues with individual privacy management. In addition, it is important to understand that offering people more choices about data collection doesn't necessarily give them power over how their data is used. Because individual consent is the approach favored by regulators, even tech companies who support privacy regulation will not be able to address its limitations simply by implementing better legal compliance.

Few people have the time and capacity to continually gather up-to-date information on how their data is collected, used, and transferred between different entities.

Computer scientists might instead think about how their own processes for building products or doing research can be designed to encourage meaningful input (and yes, even refusal) from the public early on, before technology is deployed. Collective refusal approaches taken by the public are pragmatic because they rely on methods that are available to large numbers of people. However, many examples in this article rely on institutionalized power that requires privilege to access, such as the legal system, which only responds to harm after it has been done. Collective refusal is an imperfect approach, but may be a viable practical option given the lack of public trust in engineers and computer scientists. Regaining public trust by being open to change will be essential to work in technology going forward.

At the same time, computer scientists themselves often have limited power to affect change. Individual engineers at tech companies, or individual researchers working in large labs, may feel they have little influence on higher-up decisions. But as the recent movement against facial recognition demonstrates, employees presenting a united front can meaningfully speak out against harmful uses of technology from within tech companies. These efforts to have honest conversations and build relationships with co-workers can lead to real moments of change. The best thing computer scientists can do when we recognize collective refusal by the public might be to see ourselves as members of that public, living in a society we also help shape, and add our own refusal to a growing movement.

ACKNOWLEDGEMENTS

I thank my mentor and collaborator J. Nathan Matias for supporting this work. I also thank the MIT Visualization Group, and the participants of the Contested Data workshop at Data & Society, for conversations that influenced my thinking on refusal.

References

[1] Lee, C. and Zong, J. Consent is not an ethical rubber stamp. *Slate.* (August 30, 2019); https://slate.com/technology/2019/08/consent-facial-recognition-data-privacy-technology.html

[2] Solove, D. J. Privacy self-management and the consent dilemma. *Harvard Law Review* 126, 7 (2012).

[3] Benjamin, R. Informed refusal: Toward a justice-based bioethics. *Science, Technology, and Human Values 41*, 6 (2016).

[4] Buolamwini, J. We must fight face surveillance to protect Black lives. *OneZero.* (June 2, 2020); https://onezero.medium.com/we-must-fight-face-surveillance-to-protect-black-lives-5ffcd0b4c28a

Biography

Jonathan Zong is a human-computer interaction researcher pursuing a Ph.D. at the Massachusetts Institute of Technology. Zong graduated from the Visual Arts and Computer Science departments at Princeton University in 2018. He is a 2019 Paul and Daisy Soros Fellow and NSF Graduate Research Fellow.