Editors: Jens Grossklags, jens.grossklags@in.tum.de | Heather Richter Lipford, richter@uncc.edu | Jessica Staddon, jessica.staddon@gmail.com

Privacy for the People? Exploring Collective Action as a Mechanism to Shift Power to Consumers in End-User Privacy

Sauvik Das, W. Keith Edwards, DeBrae Kennedy-Mayo, Peter Swire, and Yuxi Wu | Georgia Institute of Technology

How might we use computer-supported collective action to hold data aggregators accountable to the individuals whose data they collect and monetize? In this article, we outline a vision for computer-supported collective action in the context of end-user privacy.

First-party and third-party personal data aggregators increasingly employ sophisticated tracking and profiling technologies to create and monetize detailed digital portraits of users at-scale.[1] These technologies can thwart users' attempts at curtailing them; for example, even if users attempt to take steps such as restricting cookie settings to mitigate tracking, techniques such as browser fingerprinting still provide ways for data aggregators to track individuals and their behaviors across the Internet.[2] Moreover, this tracking and consolidation of personal data are all done outside of users' direct awareness and without informed consent, often with these practices hidden within terms of service and privacy policy agreements that are notoriously opaque. In short, today, data aggregators have limited accountability to the individual users whose data they collect and monetize.

Digital Object Identifier 10.1109/MSEC.2021.3093135
Date of current version: 3 September 2021

How might we hold data aggregators accountable to the people—i.e., the users whose data they collect and monetize?

While top-down regulation may provide some rebalance, there are other approaches that are more grassroots in nature, and history provides examples from the past that may inform paths forward today. In particular, there are parallels between the state of digital privacy today and labor in the beginning of the industrial age. In the early industrial age, strategies employed by powerful and well-funded institutions required (and disproportionately benefited from) the contributions of individual workers. As individuals, these workers had little ability to change the system due to the overwhelming power imbalance between them and their employers. Legal doctrines reinforced the property rights of employers over the ability of employees to organize—indeed, many of the early enforcement actions under the Sherman Antitrust Act of 1890 were used on behalf of employers to break alleged "monopolies" of workers seeking to strike.

Gradually, however, the Progressive era saw progress for worker and consumer protections vis-à-vis the large corporations. Collective action by workers was matched with political action on behalf of workers and consumers, such as limited work weeks, pay increases, and the Food and Drug Act of 1906. These Progressive era reforms expanded during the 1930s, with protections for labor union collective action guaranteed by the Norris-LaGuardia Act of 1930 and the Wagner Act of 1935. One result was greater income equality in the United States—scholars have termed the period from 1937 to 1947 the "Great Compression" to describe the sharp fall of income inequality compared to the earlier period of the "Robber Barons." By 1947, more than a third of nonfarm workers were union members (https://en.wikipedia.org/wiki/Income_inequality_in_the_United_States).

In short, collective action—be it in the form of labor unions, grassroots

 Copublished by the IEEE Computer and Reliability Societies

collectives, or other organizational forms—can serve as a mechanism to shift power and increase the accountability of large, organized institutions to the individuals over which they have control and can even help develop law and regulatory action to support this shift. Such collective action has not only been employed in the context of labor but also as a means of other political change. Forms of "computer-supported collective action" (CSCA), for example, helped to organize the Arab Spring, Occupy, Indignados, and other political and social justice movements.[3] In the context of privacy, CSCA provided the impetus that led to regulatory frameworks such as the California Consumer Protection Act (CCPA).

Yet, despite the potential of CSCA as a mechanism to shift power, the vast majority of CSCA efforts fail. As social computing platforms have proliferated across the Internet, a corresponding body of knowledge has steadily accumulated about how such platforms can be used to foster and formalize successful CSCA efforts. This body of knowledge has explored, e.g., strategies for grassroots organization of crowd-workers to negotiate better terms for their work.[4]

Privacy is a particularly challenging domain for CSCA for a number of reasons. First, for most of us, privacy is a secondary concern: while most of us desire the property of privacy in our use of computing systems, privacy is external to and distinct from our day-to-day tasks in using those computing systems. Second, different people have different understandings of what may constitute a privacy harm; for example, studies comparing teens to adults have shown a generational difference in orientations toward privacy violations. Third, given the information asymmetries in what data are collected about users, how it is used, what it is worth, and so on, actionable privacy demands—that are effectuated through legal and regulatory frameworks as well as the functionality of Internet services themselves—may be difficult to shape without expert stewardship. Finally, while some data aggregators (e.g., Facebook) are directly impacted by consumer action, others (e.g., Equifax) are not. We term the former *data aggregators subject to collective action* (*DASCAs*) and focus on these institutions in our discussion.

In this article, we explore the foreseen technical and legal challenges and opportunities of creating a CSCA system—Privacy for the People (PftP)—to help Internet users construct publics in search of greater privacy protections and accountability from DASCAs. Doing so requires integrated research and analysis from both the technical and legal perspectives. From the technical perspective, we must develop tools that facilitate coordination and action across grassroots collectives of users. From the legal perspective, we must explore legal doctrines and institutions through which grassroots privacy collective action might be stewarded to create enduring change in privacy practices. Technical solutions must work with the legal frameworks that exist where they are deployed. And likewise, legal frameworks must be flexible in the face of an ever-changing landscape of technical innovation.

Background

Collective action is "action taken by multiple people in the pursuit of the same goal or collective good."[5] CSCA is the use of computing to facilitate collective action, e.g., by constructing publics, facilitating communication about problems and solutions, and then helping coordinate toward group action.

In the context of privacy, there is evidence that CSCA can work, especially when legal rules and institutions support and align with such efforts. For example, a 2017 petition signed by over 385,000 California residents was the origins of today's CCPA. For the 2020 California Privacy Rights Act ballot initiative, over 900,000 individuals signed the official petition to the state (https://ballotpedia.org/California_Consumer_Personal_Information_Disclosure_and_Sale_Initiative_2018). Other petition efforts, however, fall short of effecting real change: for example, a Change.org petition responding to the Cambridge Analytica scandal generated nearly 180,000 signatures, but did not result in any material redress. Similarly, over 243,900 people responded to a petition seeking redress after the 2017 Equifax data breach: the petition "Don't let EQUIFAX escape liability!" (https://www.change.org/p/don-t-let-equifax-escape-liability), addressed to the Federal Trade Commission. Yet, over three years after the event, people are still signing this petition, suggesting that adequate amends have not been made.

What differentiates CSCA efforts that succeed versus those that fail? Part of the answer is technical, and part of the answer is based on law and institutional design.

Technical

Shaw et al.[5] introduced a five-phase lifecycle for CSCA that helps diagnose the technical shortcomings of existing CSCA systems. The patterns in this lifecycle recur across a number of systems designed to support end-to-end collective action and constitute the stages of a coordinated effort. Briefly, these five stages are: 1) identify a problem and others who care about it; 2) generate, debate, and select viable solutions; 3) coordinate and prepare for action; 4) take action; and 5) assess, document, and follow up. Shaw et al.'s analysis shows how technical systems can support each of these phases, but they also argue that campaigns tend to break down at the transition between phases of action, especially when collectives need to transition between systems to go from one phase of the lifecycle to another—e.g., from constructing a public on Change.org, to identifying demands on reddit, to mobilizing and acting in the physical world. In the Equifax petition example, after

signing a petition and helping bring attention to a problem, signers had no way to collectively debate on the exact mechanics of what solution they wanted from Equifax, and no coordinated way to act to express their discontent. Even a system that perfectly transitions collectives through the CSCA lifecycle, however, might be considered just the tip of the iceberg of what Ford calls a broader "architecture for digital democracy" that requires, prior to the deliberative practices outlined by Shaw et al.,[5] equitable access to high quality information and protection against Sybil attacks.[6]

Law and Institutional Design

In the case of the Equifax petition, there was also no obvious mechanism to legally demand or otherwise influence Equifax to act once the group had reached conclusions about its preferences. In contrast, in the case of CCPA, the California state constitution permits ballot initiatives, which can help translate a popular petition into law. More generally, there exist multiple possible institutional models for how a group may organize itself to achieve lasting privacy-protecting collective action through existing legal structures.

One such structure might be a user cooperative in which multiple individual users can unite to improve their bargaining position. For instance, Great Plains farmers have formed sellers' cooperatives to assist in selling their wheat, and consumers have formed buyers' cooperatives for grocery stores. Another salient institutional structure may be the appointment of a privacy fiduciary for large collectives. A fiduciary is someone, such as the executor of a will, who owes a duty of loyalty to protect the interests of someone else, such as the beneficiaries of a will. Applied to online commerce, the fiduciary approach would require a DASCA to apply privacy practices in the best interest of individual consumers. Note that the U.S. legal mechanism of a union would not appear to be well suited to consumers organizing against DASCAs. In the United States, the National Labor Relations Act applies to "labor"—meaning actual work performed. Whatever the institutional mechanism used to strengthen the bargaining position of consumers, a wide range of technical mechanisms might inform the DASCA about what the people want.

Envisioning Privacy for the People

How can we combine these technical and legal perspectives to improve CSCA as a mechanism to shift power to consumers in end-user privacy, and hold DASCAs accountable to those whose data they collect and monetize?

Technical Considerations

From the technical perspective, our vision is to design and evaluate PftP as an end-to-end, participatory CSCA system that helps congregate and shepherd publics to wage a coordinated digital protest campaign against a DASCA. We envision PftP as an independent social platform through which users can connect with each other and participate in protest campaigns that transition protest campaigns through the first four phases of CSCA outlined by Shaw et al.[5]

1. *Identifying a problem*: Systems that support this phase should "encourage connection, expression and listening."[5] Prior work suggests that this phase of CSCA is primarily facilitated through social networking platforms like Facebook, Twitter, and Instagram.[3] But can these platforms be trusted when they are the ones being protested *against*? Moreover, while these platforms have been successfully appropriated to support grassroots collective action, they are designed for general purpose, contextually agnostic sharing—this allows for broad reach but there is often contextual misalignment between what an organizer might be requesting and what a reader might be receptive toward. What is needed is a platform that facilitates the construction of publics—or collectives that arise from, and in response to, specific issues that are qualified by the context in which they are experienced.[7] We envision PftP as providing a "semipublic" congregation grounds—the equivalent of a public sidewalk in front of a store—in which users can view socially and contextually-relevant digital protests as they browse the web.
2. *Generating, debating, and selecting viable solutions*: In this phase, PftP must facilitate the "structured gathering of ideas" and shepherd the collective toward convergence on the best ideas.[5] However, this bottom-up percolation of ideas must be carefully scaffolded to assure productive forward momentum. In prior work exploring how crowd-workers on Amazon's Mechanical Turk can collectively bargain for fair wages and work practices, Salehi, Irani, and Bernstein discovered two oppositional challenges—stalling and friction—when designing a collective action platform designed to increase the collective bargaining strength of grassroots publics.[4] Stalling entails a loss of momentum: a public would form around an issue but, without any tension or clarity in driving toward consensus, would quickly disassemble without acting. Friction entails an impasse in which two or more opposing ideas lead to a break down in civil discourse and progress. To overcome these challenges, the authors offer a series of design suggestions, e.g., setting clear deadlines for consensus, allowing for decisions to move forward with space for undoing if necessary, encouraging reflection and producing hope. Complementarily, in an analysis of participatory

governance on social media, Engelmann, Grossklags, and Herzog note the importance of protecting against manipulative actors and ensuring secure, verifiable, and auditable voting processes.[8] We envision PftP as providing moderated fora to securely shepherd publics through the generation, debate, and selection of both salient privacy harms and demands for redress and change.

3–4. *Coordinating, preparing, and taking action*: In these two phases, a CSCA system should help a public exert its collective bargaining power against a DASCA until their demands are met. But what might "action" look like? Van Laer and Van Aelst[9] introduced a "typology of digitalised action" for cyberprotest, distinguishing between Internet-supported and Internet-based protest tactics, where the former is leveraging the connective potential of the Internet to mobilize action in the physical world (as exemplified, e.g., by the Arab Spring or the Occupy movements), and the latter is scoped strictly online (e.g., online petitions and "hacktivism"). More recently, Vincent et al.[10] introduced a typology for "data leverage"—or actions the public can take to disrupt or harm the operations of DASCAs—that spans data strikes, data poisoning, and conscious data contribution. Different actions have different associated legal risks. For example, hacktivist activities are unambiguously illegal—conscripting publics to run distributed denial of service attacks, for example, will expose many in that public to legal risks. We envision PftP as supporting Internet-based protest tactics with low legal risk—e.g., digital boycotts, data strikes, social media sit-ins.

Legal Considerations

To fully realize PftP will require greater understanding of what legal frameworks can support online action, as well as the institutional forms that can most effectively help translate public demand into actionable recourse. For example, one necessary aspect of designing PftP is to minimize risk under antitrust, defamation, and other laws.

Expanding Theory for Shaw et al.'s Phase 5: At a theoretical level, Shaw et al.'s CSCA model is currently underdeveloped at its fifth and final phase—"Assess, document, and follow-up." There are numerous legal and institutional design considerations in how the group action—such as submitting a petition—may or may not result in changed privacy practices by the DASCA. To ensure effective action, there is a need to explore what institutional designs will foster effective CSCA under what conditions, as well as the interaction of bottom-up grassroots and top-down regulatory solutions.

Assessing Direct and Indirect Effects of the Effectiveness of CSCA Initiatives: One theme from prior CSCA research has been the relatively limited direct, immediate impact from collective action initiatives. Even where collective action has defined demands through petitions or other collective action, it has often appeared that the petition has been ignored—the DASCA has often not responded directly to such demands with changed practices. Part of this perceived nonimpact may be because it is rare for a short-term call for change, such as 30–60 days, to result in an immediate and visible change in behavior by a DASCA. On the other hand, there may often be indirect and longer-term effects of collective action. For example, the Cambridge Analytica story broke in March 2018, resulting in online collective action initiatives to prompt change in Facebook practices. Despite limited immediate changes in Facebook practices, the Federal Trade Commission (FTC) announced in July 2019 that Facebook would pay a fine of US$5 billion and make what the FTC chairman called "sweeping conduct relief" in its privacy practices (https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions). A key challenge, then, will be for publics to assess and track progress over extended periods of time despite the more "acute" nature of CSCA campaigns.

How might we use CSCA to hold data aggregators accountable to the individuals whose data they collect and monetize? Answering this question requires integrated research and analysis from both the technical and legal perspectives. From the technical perspective, we must develop systems that facilitate coordination and privacy-related collective action across grassroots collectives of users. From the legal perspective, we must explore mechanisms to steward collective action through legal doctrines and institutions that can create enduring change in privacy practices. To that end, we introduced a vision for an end-to-end participatory CSCA system to facilitate grassroots privacy collective action—Privacy for the People—and explored the legal and technical challenges thereof. We hope this article serves as a call to action for scholars in both computing and law to explore novel mechanisms through which DASCAs can be held more directly accountable to the people. ■

References

1. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. London: Profile Books, 2019.
2. G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz, "The web never forgets: Persistent tracking mechanisms in the wild," in *Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Security*, pp. 674–689. doi: 10.1145/2660267.2660347.

3. W. L. Bennett and A. Segerberg, "The logic of connective action: Digital media and the personalization of contentious politics," *Inf, Commun. Soc.*, vol. 15, no. 5, pp. 739–768, 2012. doi: 10.1080/1369118X.2012.670661.
4. N. Salehi, L. C. Irani, M. S. Bernstein, A. Alkhatib, E. Ogbe, and K. Milland, "We are dynamo: Overcoming stalling and friction in collective action for crowd workers," in *Proc. 33rd Annu. ACM Conf. Human Factors Comput. Syst.*, 2015, pp. 1621–1630.
5. A. Shaw et al., "Computer supported collective action," *Interactions*, vol. 21, no. 2, pp. 74–77, 2014. doi: 10.1145/2576875.
6. B. Ford, "Technologizing democracy or democratizing technology? A Layered-Architecture perspective on potentials and challenges," in *Digital Technology and Democratic Theory*, Chicago, IL: Univ. of Chicago Press, 2021, pp. 274–321.
7. C. DiSalvo, "Design and the construction of publics," *Design Issues*, vol. 25, no. 1, pp. 48–63, 2009. doi: 10.1162/desi.2009.25.1.48.
8. S. Engelmann, J. Grossklags, and L. Herzog, "Should users participate in governing social media? Philosophical and technical considerations of democratic social media," *First Monday*, vol. 25, no. 12, 2020. [Online]. Available: https://journals.uic.edu/ojs/index.php/fm/article/view/10525, doi: 10.5210/fm.v25i12.10525.
9. J. Van Laer and P. Van Aelst, "Cyber-protest and civil society: The Internet and action repertoires in social movements," in *Handbook of Internet Crime*, J. Yvonne and M. Yar, Eds. Milton: Willan, 2013, pp. 248–272.
10. N. Vincent, H. Li, N. Tilly, S. Chancellor, and B. Hecht, "Data leverage: A framework for empowering the public in its relationship with technology companies," in *Proc. 2021 ACM Conf. Fairness, Accountability, Transparency*, pp. 215–227.

Sauvik Das is an assistant professor of interactive computing, cybersecurity, and privacy at Georgia Tech, Atlanta, Georgia, 30332, USA, where he directs the Security, Privacy, Usability and Design Lab. His research centers on the question: How can we shift power in end-user privacy away from surveillance institutions and toward the people? Das received a Ph.D. in human–computer interaction from Carnegie Mellon University. His work has been widely recognized, including with three Best Paper Honorable Mention Awards at the Association for Computing Machinery (ACM) CHI, a Best Paper Award at ACM Ubicomp, a Distinguished Paper Award at the Symposium on Usable Privacy and Security. Contact him at sauvik@gatech.edu.

W. Keith Edwards is a professor of interactive computing at Georgia Tech, Atlanta, Georgia, 30332, USA, where he directs the GVU Center. Prior to joining the faculty at Georgia Tech he was a principal scientist at Xerox PARC where he led the Ubiquitous Computing area. His primary research interest is in human–computer interaction, especially as applied to core computing concerns such as security and networking. Edwards received a Ph.D. in computer science from Georgia Tech. Contact him at keith@cc.gatech.edu.

DeBrae Kennedy-Mayo is a faculty member at the Georgia Tech Scheller College of Business, Atlanta, Georgia, 30332, USA. Kennedy-Mayo received a J.D. from Emory University School of Law. She serves as part of a small team at Georgia Tech, headed by Peter Swire, that engages in research on legal and policy issues concerning privacy and cybersecurity. Kennedy-Mayo is also a senior fellow with the Cross-Border Data Forum. Swire and Kennedy-Mayo are the coauthors of the 2020 edition of *U.S. Private Sector Privacy: Law and Practice for Information Privacy Professionals*. Contact her at debrae.kennedy-mayo@scheller.gatech.edu.

Peter Swire is the Elizabeth and Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business, Atlanta, Georgia, 30308, USA, senior counsel with Alston & Bird LLP, Atlanta, Georgia, 30309, USA, and Research Director for the Cross-Border Data Forum, Atlanta, Georgia, 30309, USA. Swire received a J.D. from the Yale Law School. In 2015, the International Association of Privacy Professionals awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Under President Clinton, Swire was the Chief Counselor for Privacy, the first person to have U.S. government-wide responsibility for privacy policy. Contact him at pswire3@gatech.edu.

Yuxi Wu is a Ph.D. student in computer science at Georgia Tech's School of Interactive Computing, Atlanta, Georgia, 30332, USA, advised by Sauvik Das and Keith Edwards. Wu received an M.S. in computational analysis and public policy from the University of Chicago and is working toward her Ph.D. in computer science at Georgia Tech. Prior to starting her Ph.D., she was a data scientist for grassroots fundraising with the Democratic National Committee. Contact her at yuxi@gatech.edu.