2018

The Case Against Idealising Control

Woodrow Hartzog
Boston University School of Law

The Case Against Idealising Control

*Woodrow Hartzog**

Every year on the first day of my course on information privacy law, I begin by asking each of my students to give me their definition of 'privacy.' Their answers wouldn't surprise you—many say something like 'things that are secret,' 'sensitive information,' and 'things shared in confidence.' But every year one conceptualisation of privacy dominates the conversation: privacy as '*control* over our personal information.'

My students aren't the only ones who think this way. Ostensibly, nobody can agree on a singular definition of privacy.[1] I've argued as much on several occasions.[2] However, a closer inspection reveals the truth: most people in industry and policy think of privacy and data protection in terms of control.[3]

Let's look at the evidence. Mark Zuckerberg testified on behalf of Facebook that 'We believe strongly in providing meaningful privacy protections to people. This is why we work hard to communicate with people about privacy and build controls that make it easier for people to *control* their information on Facebook.'[4] Bill Gates wrote for Microsoft that

> Users should be in *control* of how their data is used. Policies for information use should be clear to the user. Users should be in *control* of when and if they receive information

DOI: 10.21552/edpl/2018/4/5

* Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University. The author would like to thank Miranda Jang, Amy Hahn, and Kristen Annunziato for their excellent research assistance.

1 Daniel Solove, *Understanding Privacy* (First Harvard University Press 2008).

2 Woodrow Hartzog and Neil Richards, 'Taking Trust Seriously in Privacy Law' [2016] 19 Stanford Technology L Rev 431; Woodrow Hartzog and Neil Richards, 'Privacy's Trust Gap' [2017] 126 Yale L J 1180; Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018).

3 I recognize the theoretical, jurisprudential, and practical distinction between privacy and data protection, particularly in Europe. However, in this opinion I will refer to them synonymously insofar as both of them refer to the rules about how personal information is collected, used, processed, and shared. For more information, see also Juliane Kokott and Christoph Sobotta, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' [2013] 3/4 IDPL 222-228 <https://doi.org/10.1093/idpl/ipt017> accessed 23 November 2018.

4 Mark Zuckerberg's written testimony for House Energy and Commerce Committee hearing on 11 April 2018 <https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf> (*note*: the word 'control' is mentioned over 1,000 times). It goes on like this for a while. See also Dan Fletcher, 'How Facebook is Redefining Privacy' (*Time*, 20 May 2010) <http://content.time.com/time/magazine/article/0,9171,1990798-4,00.html> accessed 23 November 2018 ('The way that people think about privacy is changing a bit ... What people want isn't complete privacy. It isn't that they want secrecy. It's that they want control over what they share and what they don't.'); Anita Balakrishnan, Matt Hunter and Sara Salinas, 'Mark Zuckerberg Has Been Talking About Privacy for 15 Years – Here's Almost Everything He's Said' (*CNBC*, 21 March 2018) <https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html> accessed 23 November 2018 ('When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key.'); Emily Stewart, 'The Privacy Question Mark Zuckerberg Kept Dodging' (*Vox*, 11 April 2018) <https://www.vox.com/policy-and-politics/2018/4/11/17225518/mark-zuckerberg-testimony-facebook-privacy-settings-sharing> accessed 23 November 2018. (Every time that a person chooses to share something on Facebook, they're proactively going to the service and choosing that they want to share a photo, write a message to someone, and every time, there is a control right there, not buried in settings somewhere but right there when they're posting, about who they're sharing with[.]').

> to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.[5]

The entire tech industry seems to have reached a consensus that privacy is, in fact, all about control.[6] Many scholars agree.[7] Even professional organisations and privacy advocates embrace the concept of control.[8]

But it's not just scholars, industry, and privacy advocates. Lawmakers, regulators, and judges seem to have more or less settled on a notion that the key to privacy generally, and data protection specifically, is control over personal information.[9] Recital 7 of the General Data Protection Regulation (GDPR), is titled 'The framework is based on control and certainty.' It explicitly states that 'Natural persons should have control of their own personal data.'[10] The reasoning behind Europe's ePrivacy Directive is that

---

5 Bill Gates, 'Bill Gates: Trustworthy Computing' (*Wired*, 17 January 2002) <https://www.wired.com/2002/01/bill-gates-trustworthy-computing/> accessed 23 November 2018; See also Robert Lemos, 'Gates: Security is Top Priority' (*CNET*, 2 March 2002) <https://www.cnet.com/news/gates-security-is-top-priority/> accessed 23 November 2018. Current CEO Satya Nadella agrees. See also Marshall Kirkpatrick, 'Data Privacy: What Bill Gates Said 10 Years Ago' (*Readwrite*, 18 January 2012) <https://readwrite.com/2012/01/28/data_privacy_what_bill_gates_said_10_years_ago/> accessed 23 November 2018; Latil K Jha, 'Privacy Is A Human Right: Microsoft's Satya Nadella' (*BW BusinessWorld*, 8 May 2018) <http://www.businessworld.in/article/-Privacy-is-a-human-right-Microsoft-s-Satya-Nadella-/08-05-2018-148572/> accessed 23 November 2018. ('We are focused on three core pillars, first privacy. Privacy is a human right. We at Microsoft have enshrined a set of principles that ensure that we preserve this human right, protect this human right ... We ensure that when we use data, it is to benefit the user. We ensure that the user is always in control of their data and its use.').

6 See, eg Nicholas Thompson, 'Jack Dorsey on Twitter's Role in Free Speech and Filter Bubbles' (*LinkedIn*, 17 October 2018) <https://www.linkedin.com/pulse/jack-dorsey-twitters-role-free-speech-filter-bubbles-thompson> accessed 23 November 2018. (Jack Dorsey, Twitter CEO, during interview at Wired 25th Anniversary Festival said 'I do believe that individuals should own their data and should have the right to have the controls over how a company might utilize that and how a service might utilize that and be able to pull it immediately.'); Andrew DeVore, in written testimony to US Senate Committee on Commerce, Science, and Transportation for September 26, 2018 hearing <https://www.commerce.senate.gov/public/_cache/files/7c30e97b-e5fb-49cc-806e-5cd126ee91dc/48369EAB81D0F112CEDC5672C9AF24AB.09-24-2018devore-testimony.pdf> ('From early-stage development, we built privacy deeply into the Echo hardware and Alexa service by design, and we put customers in control.'); Bud Tribble, Written testimony to United States Senate Committee on Commerce, Science, and Transportation for September 26, 2018 hearing <https://www.commerce.senate.gov/public/_cache/files/2f5f8077-24bf-4a46-9156-c44913152d47/C5C28DFD93456AAB6EE7ACAD7CBE835E.09-24-18tribble-testimony.pdf> (The Apple Vice President of Software Technology wrote 'When we do collect personal information, we are specific and transparent about how it will be used. We do not combine it into a single large customer profile across all of our services. We strive to give the user meaningful choice and control over what information is collected and used.').

7 Charles Fried, 'Privacy' [1968] 77 Yale L J 475, 482 ('Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.'); Jerry Kang, 'Information Privacy in Cyberspace Transactions' [1998] 50 Stanford L R 1193, 1218 ('[C]ontrol is at the heart of information privacy.'); Frederick Schauer, 'Internet Privacy and the Public-Private Distinction' [1998] 38 Jurimetrics J. 555, 556; Richard A Posner, *'Privacy.' In The New Palgrave Dictionary of Economics and the Law* (Peter Newman (ed), Grove Dictionaries, 1998) 103, 104.

8 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Personal Data and Individual Access Control' (IEEE) 93 <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_personal_data_v2.pdf> accessed 23 November 2018 ('As society moves towards complete connectivity, humans will require tools and mechanisms to enable agency and control over how their personal data is collected and used.'); Estelle Massé, 'Data Protection: Why it Matters and How to Protect It' (*AccessNow*, 25 January 2018) <https://www.accessnow.org/data-protection-matters-protect/> accessed 23 November 2018; Corynne McSherry, 'Data Privacy Policy Must Empower Users and Innovation' (*Electronic Frontier Foundation*, 4 April 2018) <https://www.eff.org/deeplinks/2018/04/smarter-privacy-rules-what-look-what-avoid> accessed 23 November 2018 ('Social media platforms must ensure that users retain control over the use and disclosure of their own data, particularly data that can be used to target or identify them.'); Jessica Guynn, 'After Facebook Hearings, Users Want to Know: Who Is Protecting My Data?' *USA Today* (United States, 12 April 2018) <https://www.usatoday.com/story/tech/2018/04/11/after-facebooks-mark-zuckerberg-hearings-users-want-know-who-protecting-my-data/505791002/> accessed 23 November 2018 (quoting Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, saying 'The reason we need privacy laws is precisely because individuals lose control over their personal information when it is transferred to a business[.]'); Privacy International, 'How We Use and Protect Your Data' (*Privacy International*, May 2018) <https://privacyinternational.org/basic-page/618/how-we-use-and-protect-your-data> accessed 23 November 2018 ('Privacy International strongly believes that you have the right to control the use of your personal information, and that your privacy must be respected.').

9 *DOJ v Reporters Comm. For Freedom of the Press* 489 US 749, 763 (1988); Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (The U of North Carolina Press 1995) ('[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.'); ibid 4 ('[T]he definition of privacy that has provided the basis for most policy discussions in the United States, namely that privacy is the right to control information about and access to oneself').

10 recital 7 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1. The framework is based on control and certainty.

> [T]he Regulation enhances end-user's control by clarifying that consent can be expressed through appropriate technical settings.'[11] California's new Consumer Privacy Act of 2018 provides that 'Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.[12]

The list goes on.[13]

Some scholars have recognized the limitations of control as a conceptualisation of privacy.[14] Paul Schwartz has argued that 'the critical problem with the model of privacy-as-control is that it has not proved capable of generating the kinds of public, quasi-public, and private spaces necessary to promote democratic self-rule.'[15] Specifically, he argued that thinking of privacy in terms of control either leads people to think they are acting more autonomously than they really are, or

> collapses completely in the face of the weighty reasons in support of revealing personal information. The danger is one that a belief in the virtue of self-reliant data control cannot acknowledge: information processing itself can undermine an individual's ability to participate in social and political life.[16]

They warned us, and we didn't listen. Now an empire of data protection has been built around the crumbling edifice of control.

The problem is not just that the idea of privacy as control has shortcomings or isn't up to the job. It's far worse. The idealisation of control in modern data protection regimes like the GDPR and the ePrivacy Directive creates a pursuit that is actively harmful and adversarial to safe and sustainable data practices. It deludes us about the efficacy of rules and dooms future regulatory proposals to walk down the same, misguided path.

---

11 Reasoning, Option 3, 2017/0003 (COD) Proposal.

12 The California Consumer Privacy Act, AB375, s2(a) (23 September 2018).

13 See John Kennedy, 'Data chief Helen Dixon: "Tech is crashing against social norms"' [*Silicon Republic*, 7 November 2018] <https://www.siliconrepublic.com/enterprise/dpc-helen-dixon-interview-tech-society> accessed 23 November 2018 (quoting Helen Dixon, Ireland's Data Protection Commissioner, in Silicon Republic on 7 November 2018 saying '[When it comes to privacy and phone numbers], as with many areas of data protection, it is an issue of consumer choice to control in what circumstances they want their number displayed and so on.'). See also 'UK ICO Releases Code on Data Sharing' [*Hunton, Andrews, Kurth, Privacy & Information Security Law Blog*, 12 May 2011] <https://www.huntonprivacyblog.com/2011/05/12/uk-ico-releases-code-on-data-sharing/> accessed 23 November 2018 (quoting - Christopher Graham, UK Information Commissioner, in 2011 'The public rightly want to remain in control of who is using their information and why, and they need to feel confident that it is being kept safe.'); Mark Halper, 'Isabelle Falque-Pierrotin: Privacy Needs to Be the Default, Not an Option' [*Wired*, June 2015] <https://www.wired.com/brandlab/2015/06/isabelle-falque-pierrotin-privacy-needs-default-not-option/> accessed 23 November 2018 (quoting Isabelle Falque-Pierrotin, former Chair of Article 29 Working Party, in Wired in 2015 saying '[Delisting is so important because] It gives the possibility to each of us not to alter the past but to have the possibility to control a little bit what we have done in the past and their digital appearance.'); Ann Cavoukian 'Privacy Controls Must Be Placed Back Into the Hands of the Individual' [*Globe and Mail*, 27 March, 2018] <https://www.theglobeandmail.com/opinion/article-privacy-controls-must-be-placed-back-into-the-hands-of-the-individual/> accessed 23 November 2018 (The former three-term Information and Privacy Commissioner of Ontario argued 'We must take back control of our personal information from organizations and place it in the hands of the data subject, where it belongs... Now you will be in the driver's seat. You will be in control – privacy is all about control!').

14 See eg, Solove, *Understanding Privacy* (n 1); Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012) 148. See also Daniel Solove 'Privacy Self Management and the Consent Paradox' [2013] 126 Harvard L Rev 1880.

15 Paul Schwartz 'Privacy and Democracy in Cyberspace' [1999] 52 Vand L Rev 1609, 1661.

16 ibid 1663.

In fact, except in a few rare instances, I argue that we should dislodge and minimise the concept of control as a goal of data protection.

I'm guilty of it too. In the past I've advocated for more control over personal information.[17] I've sought private law approaches that might empower data subjects and meaningfully mitigate data abuses. I now realise that I was asking far too much from a concept that works best when preserved, optimised, and deployed in remarkably limited doses. Our personal agency is required for control to work and, after all, we are only human. The concept of control is far too precious and finite to meaningfully scale. It will never work for personal data mediated by technology.

Now at this point you might be saying to yourself, 'Well, sure, if the control is conditional, vague, uniformed, and contingent upon action, then of course it's no good. But our industry/framework/goal is different—we advocate for *real* control.' This kind of idealised control is impossible in mediated environments. Here's why:

First, control is illusory. It's a bit of a shell game. That's because the control we are given online is mediated, which means it cannot help but be engineered to produce particular results. When it comes to control, design is everything. The realities of technology at scale mean that the services we use must necessarily be built in a way that constraints our choices. Imagine a world where every user got to dictate their own terms in an open text box instead of a boilerplate terms of use. Companies would never get off the ground. Instead, we get boxes to check, buttons to press, switches to activate and deactivate, and other settings to fiddle with.

In theory, control serves our autonomy. It respects peoples' choices. When we are in control, we are relatively free. The problem with respecting everyone's personal commitments is that for-profit tech companies have their own agendas. They want users to be maximally forthcoming to monetise all this information. Hence, it is to their advantage to make users believe they have more control than they are actually given.

Furthermore, personal views of privacy are subject to change. Hence, tech companies have an incentive to re-engineer privacy preferences so that people who aren't maximally disclosing come to share more and more information.[18] A good strategy for accomplishing this is giving users the illusion that they are freely changing their minds, fully aware of the costs and benefits. Such knowledge, of course, never exists; it's information asymmetries from here to the end of time.

Our mediated perception of control obscures the fact that design funnels behaviour. People can only click on the options that are provided to them. Ethicist Tristan Harris has written

17 Woodrow Hartzog 'Chain-Link Confidentiality' [2012] 46 Georgia L Rev 657.

18 See, eg, Brett Frischmann and Evan Selinger, *Re-Engineering Humanity* (Cambridge University Press 2018); Hartzog, *Privacy's Blueprint* (n 2).

> Western Culture is built around ideals of individual choice and freedom. Millions of us fiercely defend our right to make 'free' choices, while we ignore how those choices are manipulated upstream by menus we didn't choose in the first place.[19]

According to Harris,

> This is exactly what magicians do. They give people the illusion of free choice while architecting the menu so that they win, no matter what you choose… By shaping the menus we pick from, technology hijacks the way we perceive our choices and replaces them with new ones.[20]

We give this fake control to our kids often, such as when I give my kids a choice between going to the park or the movies. They feel empowered and I avoid a trip to the pet store so I can stave off a conversation about a new puppy for one more week.

Design also nudges us by sending us signals and making tasks easier or harder to encourage us to act in predictable ways. Companies deploy 'dark patterns' to exploit our built-in tendencies to prefer shiny, colourful buttons and ignore dull, grey ones. They may also shame us into feeling bad about withholding data or declining options. They might simply make exercising control possible but costly through forced work, subtle misdirection, and incentive tethering.[21]

Sometimes we get wheedled into oversharing simply through the design of online services. Platforms design systems to make sharing feel good, such as encouraging us keeping a 'streak' going in Snapchat or nudging us to share old posts or congratulate others on Facebook. In addition, platforms make sharing so damn *easy*. The key to keeping the data spigot flowing is to get people to *want* to say yes and to require the least amount of effort for them to impulsively do so. Desire has powerful tendency to dampen scepticism. If we users want it bad enough, we can rationalise any decision.

The control we get in mediated environments will always be somewhat illusory, even if companies make every effort to make that control meaningful. That's because they can't do anything about the fact that exercising control requires choosing, and those choices must be architected. Cass Sunstein wrote

> When people make decisions, they do so against a background consisting of choice architecture. A cafeteria has a design, and the design will affect what people choose to eat. The same is true of websites. Department stores have architectures, and they can be de-

19 Tristan Harris, 'How Technology is Hijacking Your Mind—from a Magician and Google Design Ethicist' (*Medium*, 18 May 2016) <https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3> accessed 23 November 2018.

20 ibid.

21 For more information on the concept of dark patterns, see Harry Brignull's <http://www.darkpatterns.org>.

> signed so as to promote or discourage certain choices by shoppers (such as leaving without making a purchase).[22]

This architecture will affect people's choices even if the effect is not intended by designers. For example, people have a tendency to buy things in a store they encounter first, so even if you are not trying to sell a lot of a chocolate, putting candy bars at the entrance to your store will probably move more sweets than if you tucked them away in some corner.

We cannot avoid choice architecture. Sunstein wrote,

> Human beings (or dogs or cats or horses) cannot wish [choice architecture] away. Any store has a design; some products are seen first, and others are not. Any menu places options at various locations. Television stations come with different numbers, and strikingly, numbers matter, even when the costs of switching are vanishingly low; people tend to choose the station at the lower number, so that channel 3 will obtain more viewers than channel 53.[23]

Of course, these choices are not always harmful for us. Many of them might be quite useful. For example, lawmakers and companies should preserve user choice in the form of data subject rights like access and deletion. In the right regulatory environment, features like privacy dashboards and control panels can empower people while minimising the risk of inaction.

But asking companies to engineer user control paves the way for abuse and self-dealing at the margins. At scale, these margins matter. Even among those acting in good faith, we are left with the problem of relying on the notion of control and choice to do more work for us than it's capable of. We risk looking around at the robust new frameworks for data protection, the rules built to encourage meaningful control over personal information, patting ourselves on the back and saying 'mission accomplished,' when that isn't true. It wasn't even the right mission.

Second, control is overwhelming. To hear people tell it, control is something we can never get enough of. There seems to be no problem in privacy that cannot be remedied by chucking a few more switches, delete buttons, and privacy settings at people. Companies promise more and better controls, and then, when privacy harms happen, we collectively decide they should have turned the control knob up to eleven.[24] I must admit to doing this as well, having argued on several occasions for additional, improved privacy settings for users.[25]

---

22 Cass R Sunstein, 'The Ethics of Nudging' [2015] 32 Yale J on Reg 413, 418-22.

23 ibid.

24 With apologies to the great Nigel Tufnel.

25 Woodrow Hartzog, 'Social Media Needs More Limitations, Not Choices' (*Wired*, 12 March 2015) <https://www.wired.com/2015/04/social-media-needs-limitations-not-choices/> accessed 23 November 2018; Woodrow Hartzog and Evan Selinger, 'Facebook's Failure to End "Public by Default"' (*Medium*, 7 November 2018) <https://medium.com/s/story/facebooks-failure-to-end-public-by-default-272340ec0c07> accessed 23 November 2018.

Control over personal information is attractive in isolation. Who wouldn't want more power over things that affect our lives? But with this power often comes a practical obligation. If you do not exercise that control, you are at risk. Companies can take your inaction as acquiescence. As I've written elsewhere,

> while you might remember to adjust your privacy settings on Facebook, what about Instagram, Twitter, Google, Amazon, Netflix, Snapchat, Siri, Cortana, Fitbit, Candy Crush, your smart TV, your robot vacuum cleaner, your WiFi-connected car, and your child's Hello Barbie?[26]

Mobile apps can ask users for over 200 permissions and even the average app asks for about five.[27] The problem with thinking of privacy as control is that if we are given our wish for more privacy, it means we are given so much control that we choke on it.

Some recent strides in design rules, such as the GDPR's progressive 'data protection by design and by default' mandate, have mitigated some of the harm that comes from overwhelming users with choices. However, even if the default works, demands are still being made of us to make us relent.[28] Anyone that has turned off notifications for apps like Facebook's Messenger can attest to the relentless, grinding requests for the user to turn them back on almost every time the app is opened. Many can relate to the experience of a child asking for candy, over and over, until the requests become too much to ignore and we give in, simply to quiet them. Willpower can feel like a finite, vulnerable, and subjective resource, and systems are designed to deplete and erode it.[29] Once our willpower and ability to make choices has been compromised, the control users have been given is meaningless.

Even if industry figures out the platonic ideal of how a company can give data subjects' control, it wouldn't solve the bandwidth dilemma. People only have twenty four hours in a day and every company wants you to make choices. Another tragedy of the commons. Even if one company (or all companies) perfected a control interface, people would still be faced with a barrage of decisions because they use multiple apps and services. Individual control over one data flow won't change the fact that the data ecosystem is vast. And it should be if the market is to be competitive. The modern data ecosystem is mind-bogglingly complex, with many different kinds of information collected in many different ways, stored in many different places, processed for many different functions, and shared with many other parties. And even if every tech com-

---

26 Woodrow Hartzog, 'Privacy and the Dark Side of Control' (*IAI News*, 4 September 2017) <https://iainews.iai.tv/articles/privacy-the-dark-side-of-control-auid-882> accessed 23 November 2018.

27 Kenneth Olmstead and Michelle Atkinson, "Apps Permissions in the Google Play Store" (*Pew Research Center*, 10 November 2015) <http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/> accessed 23 November 2018.

28 art 25 of Regulation (EU) 2016/679 on data protection by design and by default [2016] OJ L119/1. See also recital 78 of Regulation (EU) 2016/679 on appropriate technical and organisational measures.

29 See, eg, 'What You Need to Know about Willpower: The Psychological Science of Self-Control' (*American Psychological Association*) <https://www.apa.org/helpcenter/willpower.aspx> accessed 23 November 2018; John Tierney, 'Do You Suffer From Decision Fatigue?' (*New York Times Magazine*, 17 August 2011) <https://www.nytimes.com/2011/08/21/magazine/do-you-suffer-from-decision-fatigue.html> accessed 23 November 2018.

pany merged into GoogAppazonbookle, the tension between simplicity and nuance inherent in one of the most complex and fraught environments imaginable would seem irresolvable. This is because nuance gets glossed over when companies try to simplify and shorten information. Risk is either hidden through abstraction or made so explicit and voluminous we don't even know where to begin.

Finally, control is myopic. Notions of individual control don't fit well with privacy as a collective value.[30] 'Data privacy is not like a consumer good, where you click "I accept" and all is well,' wrote scholar Zeynep Tufekci.[31] 'Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices.' When privacy is thought about in such individualistic, transactional terms, peoples' sense of privacy is always being negotiated against what others value. Control has to be tempered against other values because no single privacy ideology should be supreme in a pluralistic society where other people's autonomy matters.

Furthermore, as my work with Evan Selinger on Facebook's emotional contagion scandal emphasized, networked online disclosures make individualistic conceptions of control outdated and require deeper thoughts about networked privacy—the idea that a great deal of personal information can be revealed by other people in ways that no individual can possibly control.[32]

What makes us think that the collective result of atomised decisions will be best for privacy, anyway?[33] Scholars Alessandro Acquisti, Laura Brandimarte, and George Loewenstein have noted that a large body of research shows that peoples' privacy preferences are uncertain, contextually dependent, and malleable.[34] The availability of knowledge doesn't necessarily translate into meaningfully informed decisions.

Lawmakers favour mandated disclosures, like the warnings on cigarette boxes, because they are cheap and counterbalance 'information disparity'—that is, the reality that companies often know much more than consumers regarding the wisdom of a decision.[35] But in this context, users are being asked to consider the privacy implications of each post they create—an impossibly complex calculation to make about future risks and consequences.

---

30 See, eg, Regan, *Legislating Privacy* (n 9) 212-214; Anita Allen, *Unpopular Privacy* (OUP 2011) 13; Cohen (n 14).

31 Zeynep Tufecki, 'The Latest Privacy Debacle' (*New York Times*, 30 January 2018) <https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html> accessed 23 November 2018. See also Debbie VS Kasper, 'Privacy as a Social Good' (2007) 28 Social Thought & Research 165–189; Joshua AT Fairfield and Christoph Engel, 'Privacy as a Public Good' [2015] 65 Duke L J 385-457.

32 Evan Selinger and Woodrow Hartzog, 'Facebook's emotional contagion study and the ethical problem of co-opted identity in mediated environments where users lack control' (12(1) *Research Ethics*, 2015) 35–43 <https://doi.org/10.1177/1747016115579531>. See also Scott R Peppet, 'Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future' [2015] 105 Nw U L Rev 1153.

33 Daniel Solove, 'Privacy Self Management and the Consent Dilemma' [2013] 126 Harv L Rev 1880.

34 Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and human behavior in the age of information' [2015] 347 Science 509-514.

35 See, eg, Carl Schneider and Omri Ben-Shahar, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2014).

Another problem with control is that it leaves us wanting a more firm moral anchor. Control presumptively gives people choices, autonomy, and freedom but often not in any concrete sense. Too often, idealizing control leaves designers and data subjects without much of a sense of the deeper values to be preserved by the system's purpose or design. This lack of an ethical mooring encourages ideological drift and abuse. When control is the North Star, company leaders and policy makers also aren't given much to work with when tasked with improvement. Different kinds of control seem to be valued equally or treated as a monolith. No one is sure which choices and controls are more important than others. This paves the path for rote formalism and complacency. In the absence of more articulate values, CEOs and lawmakers say 'what is needed is *more* control.' If something goes wrong, well, then, we must not have had enough control, as though that would solve the problem.

But it's not clear that more control and more choices would help us. If anything, people need fewer, *better* personal data choices driven by moral values.[36] But it's hard to rank which choices are good without a more concrete theory of what we are protecting against. This is where additional values such as trust, obscurity and autonomy, become important.[37] They give us a better roadmap for how to allocate the precious resource of control. We need an approach that incorporates multiple values and is capable of recognizing privacy as a social good. Idealising control will stymie meaningful change.

We're Using Control Like It's a Proxy. It's Time to Embrace More Direct Values. Control should not be idealised as the future of privacy because it usually gets expressed as 'choice' in a way that undercuts its own mission. Given the pathologies of mediated choice, people should have a baseline, fundamental level of protection regardless of what they choose.[38] What we have now is a system that allows companies to offload the risks of data onto their data subjects.

Justifying control measures on privacy grounds requires so much justification, so much stretching, bending, and tying ourselves in knots, that it feels like it's merely serving as a proxy for some other protection goal that's just out of reach. Control feels intuitively right and has selling power, so we use it.

But what is the result that policymakers, industry, advocates, and data subjects are *really* hoping for? Surely it can't be control for control's sake, for the reasons covered above. Control ostensibly serves autonomy, but in mediated environments involving personal data, idealising control actually seems corrosive to autonomy. Is control valuable because people have such diverse privacy preferences? Or does it just appear that way because personal data risks are virtually impossible for people to consistently assess?

36 See, eg, Barry Schwartz, *The Paradox of Choice: Why More is Less* (HarperCollins Publishers 2005).

37 For a deeper exploration into these three values, see Hartzog, *Privacy's Blueprint* (n 2).

38 See Neil Richards and Woodrow Hartzog, 'The Pathologies of Consent for Data Practices' [2019] 96 Wash U L Rev.

If data processing is so dangerous that it requires formal permission, and choices can only meaningfully be made in elusive, demanding, and bounded environments with preconditions such as 'freely given, specific, informed, retractable, and unambiguous,' then why are we allowing controllers to engage in what feels like a fiction, even under optimal conditions? Is idealising control just a contorted and indirect way to pressure companies to lay off risky data practices? If so, why not dispense with the pretence of demanding a form of control that seems destined to misdirect industry efforts towards formalistic compliance without a meaningful change in processor behaviour?

Lawmakers have more direct options. Prohibit collection outright. Mandate deletion. Get serious with purpose limitations and the concept of 'legitimate interest.' Change the nature of the relationship between users and companies entrusted with their data to one that is fiduciary in nature. Mandate non-delegable duties of loyalty, care, and honesty. In other words, because it is virtually impossible for people to be adequately informed of data risks and exert control at scale, our rules should make sure companies cannot unreasonably favour their own interests at our expense.

The case against privacy control is an appeal to more substantive and effective privacy-related values. By expanding beyond the notion of privacy as control, lawmakers would be freed to create some rules to ensure companies are trustworthy regardless of the control we are given.