The Urgency of Creating A Slippery Slope Privacy Framework

Many privacy advocates are concerned that some lauded pandemic management strategies may turn out to be shortsighted. They often use a distinct and emotionally resonant form of expression to call attention to a domino effect leading to unacceptable future outcomes: *slippery slope discourse*. This is a significant rhetorical choice: slippery slopes have a reputation for being fallacious; yet the current criticisms are coming from academic and civil society privacy experts advancing credible positions. Creating a framework for evaluating these concerns is critical to good privacy governance.

Alex Gladstein, Chief Strategy Officer at the Human Rights Foundation, characterizes contact-tracing apps as a "slippery slope" that officials can "co-opt" by "adding more invasive features."[1] He worries this trajectory might shift democracies in an authoritarian direction where citizens get color-coded based on presumptive health status (or other features) to restrict basic liberties, like the right to travel. Could this really happen? Or are such comparisons to China hyperbolic? Privacy scholars Julie Cohen, Woodrow Hartzog, Laura Moy, Ashkan Soltani, and Ryan Calo insist the analogy deserves due consideration. But currently there is no widely agreed upon way to evaluate this risk objectively.[2]

Alistair Duff, a professor of information policy, emphasizes the risk of normalization: "The coronavirus tracker apps spreading around the world may well be the proverbial slippery slope… Populations are likely to become more submissive to tracking, regimenting and general snooping by the powers that be."[3] Relatedly, Jay Stanley, ACLU Senior Policy Analyst, cautions that using drones for pandemic purposes, like monitoring whether people follow social distancing guidelines, will "acclimate people to drone surveillance."[4] Is normalization really this powerful? Or is this an exaggerated view of how easy it is to make enduring changes to people's attitudes? Before the pandemic, civil society actors described facial recognition threats in the U.S. in just this way.[5] How can we tell if this is a likely outcome with pandemic considerations factored in?

Although slippery slope claims are widespread, they remain hard to analyze. Since some are riddled with logical fallacies, many people erroneously believe that all slippery slope pronouncements are inherently flawed. Valid slippery slope declarations exist. They are real. However, constraints that vary among individuals, from gaps in knowledge to cognitive limitations, make slippery slope issues hard to firmly grasp, carefully articulate, and judiciously counter. At bottom, getting a handle on slippery slope discourse requires addressing fundamental aspects of our shared humanity: without strong training in detachment, people regularly worry about slippery slopes because humans are vulnerable to perceived threats that trigger strong emotional reactions about change.

Slippery slope studies, which span philosophical, legal, sociological, and psychological inquiry, offer conceptual tools that can help us critically analyze slippery slope discourse. Unfortunately, the interdisciplinary literature has yet to be rigorously integrated into privacy scholarship to allow for consensus assessment strategies.[6] My privacy and pandemics position

statement is that privacy policymakers need a clear and robust framework that can be used to assess the credibility (or lack thereof) of rhetorically powerful slippery slope pronouncements and to determine how to appropriately respond to significant and legitimate slippery slope threats.

The framework should answer the following fundamental questions.

1) How can legitimate slippery slope discourse be distinguished from the fallacious variety in the context of privacy analysis, especially since scholars dispute the proper form of a slippery slope argument and many biases distort (magnify or diminish) how threatening slippery slope issues appear?

2) What are the main types of legitimate slippery slope claims in the context of privacy analysis? For example, the slippery slope literature distinguishes between full-blown "slippery slope arguments" (that carefully explain what, specifically, can lead a present action to increase the likelihood that a consequential, morally undesirable outcome will occur in the future), "slippery slope worries" (that only vaguely suggest how present behavior might compromise the future, but which nevertheless identify important issues that deserve greater attention), and "slippery slope drivers" (the causal mechanisms that increase the likelihood that one action will lead to another).

3) What are the best rhetorical strategies for refuting the different types of fallacious slippery slope claims (e.g., arguments and worries) in the context of privacy analysis?

4) What are the main slippery slope drivers that can compromise privacy (e.g., normalization, mission creep, lowered transaction costs, deep regulatory gaps, overly vague policies, etc.) and how precisely can the functions and impacts of each be specified? What privacy-compromising drivers require further study to improve how accurately they can be discussed?

5) What is the best way to evaluate the tension between short-term gains (e.g., enhanced public health or more efficient services) and long-term threats to privacy in slippery slope contexts?

6) Are there specific vulnerabilities that lead to particular slippery slope problems posing especially great concern? For example, what is the significance of some privacy advocates calling for the extreme measure of a ban on facial recognition technology?

7) Should policymakers give different weight to slippery claims made by different types of privacy professionals? For example, if advocacy groups have previously made overly-emotional appeals when motivating existing supporters or recruiting news ones, or if they have a reputation for advancing uncompromising agendas, should their slippery slope claims be viewed with heightened skepticism?

8) Should policymakers give different weight to slippery slope claims about privacy based on contextual considerations concerning where they appear (e.g., in a news story as a pithy quote, in an opinion piece, in an academic article, etc.)?

9) What are the best, evidence-based approaches for resisting slippery slope drivers across the standard array of governance options (e.g, targeting soft law, hard law, norms, markets, design, or education) and how can they be combined for maximum efficacy?

Without a robust slippery slope framework, policymakers are unduly burdened when trying to consistently, fairly, and objectively evaluate many credible privacy threats in emergencies, like pandemics, as well as ordinary circumstances.

---

[1] "Coronavirus contact tracing apps were meant to save us. They won't." Matt Burgess *Wired UK* April 30, 2020. https://www.wired.co.uk/article/contact-tracing-apps-coronavirus

[2] Cohen, Hartzog, and Moy state: "Now consider the mission creep problem…If Google wanted to develop a community mobility app similar to Alipay Health Code to push out to people's phones, it could easily do so using the granular data about individual mobility that it already has." "The dangers of tech-driven solutions to COVID-19." Julie Cohen, Woodrow Hartzog, and Laura Moy. *Brookings TechStream* June 17, 2020. https://www.brookings.edu/techstream/the-dangers-of-tech-driven-solutions-to-covid-19/ Related concerns are conveyed by Ashkan Soltani (privacy researcher and technologist), Ryan Calo (Professor of Law at the University of Washington), and Carl Bergstrom (Professor of Biology at the University of Washington) convey a comparable caution in their collaborative analysis of contact-tracing technology. Emphasizing how measures that begin as voluntary choices can transform into mandatory requirements, they state: "There is also a very real danger that these voluntary surveillance technologies will effectively become compulsory for any public and social engagement. Employers, retailers, or even policymakers can require that consumers display the results of their app before they are permitted to enter a grocery store, return back to work, or use public services—is as slowly becoming the norm in China, Hong Kong, and even being explored for visitors to Hawaii." "Contact-tracing apps are not a solution to the COVID-19 crisis" Ashkhan Soltani, Ryan Calo, and Car Bergstrom *Brookings TechStream* April 27, 2020. https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/ Indeed, when Apple and Google announced the rollout of Exposure Notification Express, a software update that lets users turn on exposure notifications on iPhones without needing to download a third-party app, Soltani characterized the move as a "slippery slope." His point is that by reducing transaction costs, the companies are nudging additional public health agencies and users to adopt the platform. Doing so, in his opinion, can propel forward the shift from voluntary to mandatory adoption. See https://twitter.com/ashk4n/status/1300830015521579010?s=20 Ashkan provided explicit permission to cite this tweet.

[3] "Coronavirus: the first big test of the information age and what it could mean for privacy." Alistair S. Duff *The Conversation* May 10, 2020. https://theconversation.com/coronavirus-the-first-big-test-of-the-information-age-and-what-it-could-mean-for-privacy-138068

[4] "Technology and Liberties in the Fight Against Coronavirus." *Jay Stanley ACLU News and Commentary*. May 19, 2020. https://www.aclu.org/news/privacy-technology/technology-and-liberties-in-the-fight-against-coronavirus/

[5] For example, consider how Jennifer Lynch, Surveillance Litigation Director at the Electronic Frontier Foundation, characterizes the impact of normalization on people's views of facial recognition technology by deliberately blurring the difference between facial verification and facial identification. She contends: "It's a slippery slope from using face recognition on your phone to the government using face recognition to track us wherever we go." "Facial Recognition Is Everywhere. Here's What We Can Do About It." Thorin Klowsowski *The NY Times* July 15, 2020. https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ Relatedly, Ashley Gorski, an ACLU staff attorney insists: "If this [facial recognition] technology is normalized at the airport, it's only a matter of time before the government cites its use at airports as a basis for deploying it elsewhere." "The Government Has a Secret Plan to

Track Everyone's Faces at Airports. We're Suing." Ashley Gorski, *ACLU News & Commentary* March 12, 2020. https://www.aclu.org/news/privacy-technology/the-government-has-a-secret-plan-to-track-everyones-faces-at-airports-were-suing/

[6] The following are illustrative examples of a larger slippery slope literature. "The Mechanisms Of The Slippery Slope" Eugene Volokh *Harvard Law Review* 116, 4 (2003): 1026-1137. "The Camel's Nose Is In The Tent: Rules, Theories, and Slippery Slopes" Mario Rizzo and Douglas Whitman *UCLA Law Review* 51, 3 (2003): 539-592. "Little Brother is Watching You: New Paternalism on the Slippery Slopes" Mario Rizzo and Douglas Whitman *Arizona Law Review* 51, 3 (2009): 685-739. "Raining on the Parade of Horribles: Of Slippery Slopes, Faux Slopes, and Justice Scalia's Dissent in Lawrence V. Texas" Ruth Sternglantz *University of Pennsylvania Law Review* 153, 3 (2005): 1097-1120. "Living on a Slippery Slope" Hugh Lafollette *The Journal of Ethics* 9, 3/4 (2005): 475-499. "The Slippery Slope Arguments in the Ethical Debate On Genetic Engineering of Humans" *Douglas Walton Science Engineering Ethics* 23 (2017): 1507-1528. "Slippery Slope Arguments" Anneli Jefferson *Philosophy Compass* 9, 10 (2014): 672-680. "The Slippery Slope of Dishonesty" Jan Englemann and Ernst Fehr *Nature Neuroscience* 9, 12 (2016): 1153-1154. "Slipping on Slippery Slope Arguments" Robert Fumaglli *Bioethics* 34 (2020): 412-419.