Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 33 *XXXIII*
Number 3

Article 4

2023

The By-Design Approach Revisited: Lessons from COVID-19 Contact Tracing Apps

Mickey Zar

Niva Elkin-Koren

The By-Design Approach Revisited: Lessons from COVID-19 Contact Tracing Apps

Cover Page Footnote

* Senior Research Fellow, Tel-Aviv University Faculty of Law. ** Professor, Tel-Aviv University Faculty of Law; Faculty Associate, Berkman Klein Center for Internet and Society at Harvard University. This Research was supported by the Volkswagen Foundation under the project “Developing the socio-technical architecture method to inform policy choices in the shaping of COVID-19 digital infrastructure.” We thank Michael Birnhack, Tilo Böhmann, Fabian Burmeister, Christian Kurtz, Helen Nissenbaum, Wolfgang Schulz, Eran Toch, and Assaf Yaakov for their helpful comments on earlier drafts. We further thank the participants of the Workshop on Interdisciplinary Research in Computer Science & Law: Emerging Challenges (March 2022), Cornell Tech Digital Life Seminar (2022), the participants of the TAU Law Workshop for Law & Technology (2022), and the participants of the Public Health & COVID-19 panel at the Surveillance and Society Conference 2022, ESHCC Rotterdam. We thank Shada Samara, Omer Ein-Habar, and Yuval Tuchman for excellent research assistance.

The By-Design Approach Revisited: Lessons from COVID-19 Contact Tracing Apps

Mickey Zar[*] & Niva Elkin-Koren[**]

[*] Senior Research Fellow, Tel-Aviv University Faculty of Law.

[**] Professor, Tel-Aviv University Faculty of Law; Faculty Associate, Berkman Klein Center for Internet and Society at Harvard University. This Research was supported by the Volkswagen Foundation under the project "Developing the socio-technical architecture method to inform policy choices in the shaping of COVID-19 digital infrastructure." We thank Michael Birnhack, Tilo Böhmann, Fabian Burmeister, Christian Kurtz, Helen Nissenbaum, Wolfgang Schulz, Eran Toch, and Assaf Yaakov for their helpful comments on earlier drafts. We further thank the participants of the Workshop on Interdisciplinary Research in Computer Science & Law: Emerging Challenges (March 2022), Cornell Tech Digital Life Seminar (2022), the participants of the TAU Law Workshop for Law & Technology (2022), and the participants of the Public Health & COVID-19 panel at the Surveillance and Society Conference 2022, ESHCC Rotterdam. We thank Shada Samara, Omer Ein-Habar, and Yuval Tuchman for excellent research assistance.

INTRODUCTION

In the early days of the COVID-19 outbreak, no hope was seemingly too large to place on the shoulders of digital technologies to ensure the future of humanity.[1] Governments around the world were eager to adopt technological solutions to combat the pandemic.[2] One such technology was digital contact tracing—that is, the tracing of contacts made with COVID-19 patients to interrupt chains of infection transmission.[3] In the wake of the first outbreaks, different types of Contact Tracing Technologies (CTTs) were designed and rapidly implemented all over the globe.[4] While the last chapter of the

---

1 *See, e.g.*, David Rotman, *Why Tech Didn't Save Us from COVID-19*, MIT TECH. REV. (June 17, 2020), https://www.technologyreview.com/2020/06/17/1003312/why-tech-didnt-save-us-from-covid-19/ [https://perma.cc/2NDD-SGXB].

2 *See* Lemos et al., *Smart Pandemic Surveillance?: A Neo-Materialist Analysis of the "Monitora COVID-19" Application in Brazil*, 20 SURVEILLANCE & SOC'Y 82, 82 (2022).

3 Andrew Anglemyer et al., *Digital Contact Tracing Technologies in Epidemics: A Rapid Review*, *in* 8 COCHRANE DATABASE OF SYSTEMATIC REVIEWS 4 (2020).

4 *See* Kelly Servick, *COVID-19 Contact Tracing Apps Are Coming to a Phone Near You. How Will We Know Whether They Work?*, SCIENCE (May 21, 2020),

pandemic has yet to be written, there is a growing consensus that CTTs did not meet the high expectations they raised.[5] After a short period of anticipated success, CTTs' assimilation around the globe declined;[6] and the quest for a panacea technological remedy to govern the spread of the pandemic eventually failed.[7]

Technological solutionism—the belief that all of humanity's problems can be solved through technological intervention alone—underlies the hope for technological salvation from the pandemic.[8] Technological solutionism notably prevailed in the initial discourse around CTT design and development.[9] The belief that technology has the power to address societal problems is widely shared. Many scholars have advocated for designing systems that would embody values to which designers, users, or other stakeholders are

---

https://www.science.org/content/article/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how [https://perma.cc/F2XZ-2ZQA].

5 *See, e.g.*, Will Douglas Heaven, *Hundreds of AI Tools Have Been Built to Catch COVID. None of Them Helped,* MIT TECH. REV. (July 30, 2021); *see generally* NATALII HELBERGER ET AL., CONDITIONS FOR TECHNOLOGICAL SOLUTIONS IN A COVID-19 EXIT STRATEGY, WITH PARTICULAR FOCUS ON THE LEGAL AND SOCIETAL CONDITIONS (2021).

6 In November 2020, the average implementation rate of CT apps in various countries around the world was 20%. Tehilla Altshuler & Rachel Aridor-Hershkovitz, *From Top Down to Bottom Up*, ISR. DEMOCRACY INST. (Nov. 23, 2020), https://en.idi.org.il/articles/32932 [https://perma.cc/4A2H-7X45]. In addition, the World Health Organization's benchmark for a successful COVID-19 CT operation is to trace and quarantine 80% of close contacts within three days of a case being confirmed—a goal few countries achieved. WORLD HEALTH ORG., CONTACT TRACING IN THE CONTEXT OF COVID-19: INTERIM GUIDANCE 7 (Feb. 1, 2021), https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf [https://perma.cc/RBD6-TE8Q]; *see also* Dyani Lewis, *Where Covid Contact-Tracing Went Wrong*, 588 NATURE 384, 384 (2020).

7 Andrew Martonik, *Contact-Tracing Apps Were the Biggest Tech Failure of the COVID-19 Pandemic*, DIGITALTRENDS (Feb. 15, 2021), https://www.digitaltrends.com/mobile/contact-tracing-apps-failed-covid-19-pandemic/ [https://perma.cc/RK9D-PGAK].

8 *See* EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM 6 (2013). As argued by Morozov, technological solutionism derives from a "never-ending quest to ameliorate," while being oblivious to complex social situations and conditions. *Id.* at 5.

9 *See* Linnet Taylor, *There Is an App for That: Technological Solutionism as COVID-19 Policy in the Global North*, *in* THE NEW COMMON: HOW THE COVID-19 PANDEMIC IS TRANSFORMING SOCIETY 209, 210 (Emile Aarts et al. eds., 2021). As Linnet Taylor described it, "the most striking feature of the technological response to the pandemic has been the degree of solutionism driving it." *See also* Stefania Milan, *Techno-Solutionism and the Standard Human in the Making of the COVID-19 Pandemic*, BIG DATA & SOC'Y, Oct. 2020, at 3.

committed.[10] The *by-design* approach—that is, the belief that pre-embedding values in the design level of technology, ex-ante, will bring about the desired social consequences, and thus determine outcomes in advance—has become a cornerstone of the modern regulatory approach to technology.[11] For example, if we take an app for creating albums of users' pictures, there are plenty of design options for promoting or impeding users' privacy. Designing the app with a feature that automatically deletes pictures after twenty-four hours will generally promote privacy. On the other hand, an architecture that prevents any deletion of data, such as blockchain, might be useful for certain types of verification, but may also compromise users' privacy. As further discussed below, the by-design regulatory approach generally assumes that norms could be embedded in technological design, and therefore technology could effectively govern users' behavior, surpassing governance by legal norms.[12] While more nuanced, this approach has nonetheless driven similar hopes as to technology's power to change the world, on its own, for the better.

This paper challenges the by-design regulatory approach by exploring the case study of Contact Tracing Apps. It aims to account for the gap between the hopes that were pinned on digital technologies and the rock of reality into which they have crashed.[13] This gap, we argue, results from overestimating the regulatory power of technology and underestimating the co-influence of various regulatory

---

[10] *See, e.g.*, Mary Flanagan et al., *Values at Play: Design Tradeoffs in Socially-Oriented Game Design*, *in* ACM CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 753 (2005) ("Values in design poses a challenge to those involved in system design to adopt values as one among a set of criteria according to which system quality is judged.").

[11] Advancements in data protection regulation take pride in their commitment to values by design, focusing mainly on privacy-by-design. As an example, consider the European General Data Protection Regulation (GDPR). *GDPR Table of Contents*, GDPR.EU, https://gdpr.eu/tag/gdpr/ [https://perma.cc/23GA-78E2]. *See also About Us*, GLOBAL PRIVACY & SEC. BY DESIGN, https://gpsbydesign.org/who-we-are/ [https://perma.cc/GJR4-PAWB] (highlighting the Canadian approach led by former Information and Privacy Commissioner for Ontario, Ann Cavoukian).

[12] *See infra* notes 17–49 and accompanying text.

[13] However, some exceptions were noted in the literature. *See, e.g., Examination of The GSS Tool - Quantitative Indices*, PRIVACY ISRAEL (Nov. 29, 2020) [hereinafter Privacy Israel Report], https://www.privacyisrael.org.il/_files/ugd/06db72_1b8af78940bb4cfeb47ab6b620bf6f08.pdf [https://perma.cc/2JDW-WXG5].

pillars. To address this gap, it is necessary to adopt an ecosystem perspective on sociotechnical systems, where technological design is but one form of regulation. This perspective allows technological design to acquire a social meaning through interaction with other regulatory forces to generate a social outcome.

As discussed in this paper, the CTT case study demonstrates a major flaw of focusing exclusively on technological solutions, which overlook the critical role of other social regulatory forces. It offers a rare opportunity to compare two extreme examples of technological affordances, reflecting contradictory strategies of contact tracing. One approach deployed a voluntary, privacy-friendly, transparent, and open-source civilian technology, while the other repurposed a mandatory state surveillance system, originally designed to gather intelligence concerning homeland security.[14] Obviously, each approach raised different expectations and almost contrary sentiments. In the case of the civilian app, HaMagen ("The Shield"), it was expected that users would flock to the app store, while the use of the Israeli General Security Service's (GSS) surveillance capabilities (known as "the TOOL") over a civilian population was perceived as a possible harbinger of the end of democracy.[15] However, neither the high hopes pinned on HaMagen nor the grave fears surrounding the TOOL have materialized: the civil app's qualities have not mobilized the bulk of users to adopt, and the TOOL was gradually disarmed of its unbounded intrusive powers through a mixture of institutional efforts, including extensive judicial and parliamentary review, until it was finally banned.[16]

The CTT case study offers important lessons to policymakers. It demonstrates the fact that technology alone can neither save the world nor destroy it. It also highlights the ways in which technological affordances are shaped by social institutions, thus transforming their social outcome. This is not to say that technological affordances are not a powerful social regulator, but rather to claim that

---

[14] For the civilian technology, see *infra* notes 69–84 and accompanying text. For the state surveillance system, see *infra* notes 111–27 and accompanying text.

[15] *See, e.g.*, Avi Marciano, *Israel's Mass Surveillance During COVID-19: A Missed Opportunity*, 19 SURVEILLANCE & SOC'Y 85, 87 (2021).

[16] For HaMagen's assimilation failure, see *infra* notes 85–110 and accompanying text. For the TOOL's assimilation battle, *see infra* 128–83 and accompanying text.

technology is but one regulating actor among others in the socio-technical ecosystem. Consequently, policymakers should beware not to overestimate the power of design choices in determining social outcomes. At the same time, we are reminded of the regulatory power of law and legal institutions. The role of law in technological contexts does not amount to simply making design choices ex-ante (e.g., setting technical standards to ensure social values). Instead, the law might also play a crucial role in shaping the social consequences of technology ex-post; for example, by restricting certain uses of pre-existing technology, introducing rights and duties, or setting liability rules.

The paper will proceed as follows: Part I introduces the by-design regulatory approach. Part II describes the CTT case study, comparing two contradictory digital contact tracing strategies in the course of their development, deployment, and aftermath. It also offers a wider perspective on the issue by analyzing the co-influence of the two strategies. Part III discusses the role of market forces in shaping the social meaning of technological design.

I. THE BY-DESIGN REGULATORY APPROACH

A rich body of literature in Philosophy,[17] Critical Theory[18] and Science and Technology Studies (STS)[19] has explored how particular design choices reflect societal values. The debate regarding the politics of technology was initially phrased by Langdon Winner in 1980 as a question: "Do artifacts have politics?"[20] Famously, Winner answered in the affirmative, stressing that politics is embedded in the materiality of technological artifacts.[21] Winner featured technology as a powerful regulator of social life, setting the stage for later attempts to pre-embed desired values at the phase of designing

---

17 *See generally* ANDREW FEENBERG, ALTERNATIVE MODERNITY: THE TECHNICAL TURN IN PHILOSOPHY AND SOCIAL THEORY (1995).

18 *See* Andrew Feenberg & Patrick Feng, *Thinking About Design: Critical Theory of Technology and the Realization of Design Possibilities*, PHIL. & DESIGN 1, 9 (2008).

19 *See generally* BRUNO LATOUR, ARAMIS, OR THE LOVE OF TECHNOLOGY (Catherine Porter trans., Harvard Univ. Press 1996) (discussing prominent examples of STS).

20 Langdon Winner, *Do Artifacts Have Politics?*, 109 DAEDALUS 121, 123 (1980).

21 *Id.*

a new technology, manifested in the aforementioned "values by design" approach.[22]

Building upon this literature, scholars such as Batia Freidman[23] and Helen Nissenbaum[24] have highlighted the socio-technical implications of design choices, seeking to identify and address these issues early in the design process. Scholars have demonstrated how particular values are embedded in search engines,[25] games,[26] and machine learning systems.[27] The by-design approach was further applied in education as a training tool, seeking to shape technology—ex ante—by raising awareness among developers about the critical values choices that they are making in designing and deploying digital systems.[28] Activists too have been using technology to counter oppressive values—such as surveillance capitalism—by developing technological measures of resistance.[29]

In the legal domain, the by-design approach emerged in response to the legal challenges raised by digital technology. In the mid-90s legal scholars introduced the theoretical framework of regulation by design.[30] In his pioneering seminal paper, Joel R. Reidenberg argued

---

[22] *See* Helen Nissenbaum, *From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?*, 26 BERKELEY TECH. L.J. 1367, 1374–75 (2011) (providing a detailed explanation of the debate and its theoretical implications).

[23] Batya Friedman et al., *Sensitive Design and Information Systems, in* THE HANDBOOK OF INFORMATION AND COMPUTER ETHICS 69, 70 (Kenneth Einar Himma & Herman T. Tavani eds., 2008).

[24] Helen Nissenbaum, *Values in Technical Design*, *in* ENCYCLOPEDIA OF SCIENCE TECHNOLOGY AND ETHICS 66, 67 (2005).

[25] *See generally* Lucas D. Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16 INFORMATION SOC'Y 169, 169 (2000).

[26] *See generally* Mary Flanagan & Helen Nissenbaum, Values at Play in Digital Games (2014).

[27] *See generally* BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY (2018) (analyzing critically machine learning systems and AI).

[28] *See* Howard Middleton, *Creative Thinking, Values and Design and Technology Education*, 15 INT'L J. TECH. DESIGN EDUC. 61, 68 (2005).

[29] *See, e.g.*, Daniel C. Howe & Helen Nissenbaum, *Engineering Privacy and Protest: A Case Study of AdNauseam*, IWPE@ SP (2017) (developing a browser extension called AdNauseam [ED-NA-SI-UM] that automatically clicks on web ads to interfere with behavioral tracking and profiling by Google).

[30] *See* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 556 (1998).

that technological affordances could steer human behavior.[31] Like many legal scholars of his generation,[32] Reidenberg was puzzled by the challenges arising from the transnational environment introduced by the internet.[33] The pace of technological development has been exponential, making it increasingly difficult for traditional laws to keep up to date with technological change.[34] The online global environment was arguably challenging the legitimacy and efficiency of national law enforcement, giving rise to a new type of governance whereby information technology was employed to govern users behavior.[35] Coining the term "Lex Informatica,"[36] Reidenberg demonstrated how technological capabilities and design choices could allow users the flexibility to shape their own online experience based on their preferences. For example, technology enabling different users to adapt their content filters based on their values mitigated the tension between the one-size-fits-all norm dictated by laws of different jurisdictions and the diversity of speech norms upheld by users.[37]

In a similar vein, Lawrence Lessig coined the phrase "code is law" to describe how algorithms govern human behavior alongside more traditional forms of governance—namely law, social norms, and markets.[38] Lessig presented a key model for conceptualizing the codependency of these regulating forces, arguing that each can

---

31 *Id.*

32 *See, e.g.*, David R. Johnson & David G. Post, *Law and Borders—the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1368 (1996).

33 Reidenberg, *supra* note 30, at 562.

34 Daniel Martin Katz, *Quantitative Legal Prediction—or—How I Learned to Stop Worrying and Start Preparing for the Data Driven Future of the Legal Services Industry*, 62 EMORY L. J. 909, 922–23 (2013).

35 Reidenberg, *supra* note 30, at 579. Reflecting a social order which relies on individuals' choice, Lex Informatica might be perceived as a more legitimate form of self-governance. Moreover, since individuals presumably possess better knowledge of their own wants and needs, governance by Lex Informatica was presumably more likely to enable choices that would efficiently maximize individuals' own utility functions.

36 *Id.* at 555.

37 Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-by-Design*, 106 CALIF. L. REV. 697, 712–13 (2018). Although governments could enforce their local speech rules using technology (for example, blocking certain websites for users within their territory), other internet users could use the same technology to control, for themselves, what content to filter and what to allow.

38 LAWRENCE LESSIG, CODE: VERSION 2.0 24 (2006).

regulate activity by itself or jointly with other forces.[39] Although Lessig noted the reciprocal nature of the interaction between these regulators, the analysis of these reciprocities was left outside the scope of his model. Moreover, from Lessig's perspective, technology was perceived as an external influence on social life, determined by factors completely separate from the social sphere to which it applies.[40] This path-breaking approach to governance has given rise to a proliferation of legal scholarship seeking to gain a better understanding of the role of technology in governing human behavior.[41] The code-is-law approach was endorsed by scholars who argued that norms could be effectively embedded in architecture, and that design could be used to effectively regulate users' behavior.[42]

It has also set the ground for a by-design regulatory approach, focusing on technical standards embedded in the design to ensure compliance with societal values.[43] For instance, first introduced as a regulatory approach by Ann Cavoukian, the former Information and Privacy Commissioner for the Canadian province of Ontario, privacy by design (PbD) identified principles that encompass privacy and could be implemented proactively.[44] Privacy by design has become one of the regulatory cornerstones of the European General Data Protection Regulation (GDPR). Article 25 of the GDPR, titled "data protection by design and by default," requires the controller of

---

39 *Id*. at 123–24.

40 *See* Niva Elkin-Koren & Michael D. Birnhack, *Introduction: Law and Information Technologies, in* THE LEGAL NETWORK: LAW AND INFORMATION TECHNOLOGY, LAW, SOCIETY AND CULTURE SERIES (2011).

41 *See, e.g.*, Nissenbaum, *supra* note 22; JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); *see also* Mulligan & Bamberger, *supra* note 37.

42 *See generally* Karen Yeung, *Towards an Understanding of Regulation by Design*, *in* REGULATING TECHNOLOGIES: LEGAL FUTURES, REGULATORY FRAMES AND TECHNOLOGICAL FIXES 79 (Roger Brownsword & Karen Yeung eds., 2008); France Bélanger & Robert E. Crossler, *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems*, 35 MIS Q. 1017 (2011).

43 *See* Mulligan & Bamberger, *supra* note 37, at 698.

44 *See* ANN CAVOUKIAN, INFO. & PRIV. COMM'R ONT., PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 5 (rev. 2011), https://privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf [https://perma.cc/N6EH-DTTX].

data to integrate appropriate technical measures encompassing data protection principles into the technologies they build and use.[45]

The by-design approach has also become a golden standard for many law reform initiatives related to Artificial Intelligence (AI). Policy initiatives seeking to minimize AI's risk to social values—such as privacy, accountability, and fairness—focus on ensuring that these values are embedded into the design ex-ante.[46]

The by-design regulatory approach has now reached the mainstream, implemented widely in the technological context.[47] Yet, as demonstrated by the case study discussed next, the by-design approach is far from a panacea. Focusing exclusively on design choices presents a major flaw: it often overlooks the critical role of other regulatory forces in determining the social outcome. It is the confluence of technology and other forces that shapes the social meaning and outcome of deploying any given technology.

Lessig staged technology among the factors influencing human activity, the others being law, social norms, and the market.[48] Our case study demonstrates the significance of the interaction between the different pillars that regulate human behavior, establishing the importance of an ecosystem analysis that accounts for all regulatory forces acting simultaneously. Moreover, unlike Lessig, we argue that technology is not a "black box" but rather an internal component

---

[45] Council Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 25, 2016 O.J. (L 119) 1; *see* Christian Kurtz et al., *Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors*, 24 AM. CONF. ON INFO. SYS., NEW ORLEANS 1, 8 (2018).

[46] A telling example is the U.S. Algorithmic Accountability Act introduced by the House and Senate. *See Federal Lawmakers in House and Senate Introduce Algorithmic Accountability Act of 2022*, NAT'L L. REV. (Feb. 11, 2022), https://www.natlawreview.com/article/federal-lawmakers-house-and-senate-introduce-algorithmic-accountability-act-2022 [https://perma.cc/HC9W-3PTN]; *see also* Joshua P. Meltzer & Aaron Tielemans, *The European Union AI Act: Next Steps and Issues for Building International Cooperation in AI*, BROOKINGS (June 1, 2022), https://www.brookings.edu/wp-content/uploads/2022/05/FCAI-Policy-Brief_Final_060122.pdf [https://perma.cc/M2F2-ELVZ] (discussing the parallel European AI Act, submitted by the European commission in April 2021).

[47] *See* Cavoukian, *supra note* 44.

[48] *See* LESSIG, *supra* note 39.

of the ecosystem in which it operates, i.e., technology is endogenous to the social system. Put differently, an ecosystem approach cannot assume technological design as a given. Instead, an ecosystem approach must regard technological design as the outcome of an ongoing process of contestation and interaction with other regulatory pillars that would subsequently determine its social meaning and practical outcomes.

Our case study demonstrates the risks involved in adopting a static perspective to technology, which assumes that social values could be successfully pre-designed. Instead, we argue that the political meaning of technology emerges through the ongoing interaction between values embedded in the technology ex-ante and those shaped ex-post throughout the dynamic processes of interpretation and the constraints applied by key social forces, notably the law.[49]

II. THE TRACING APPS CASE STUDY

Since the outbreak of the global pandemic, COVID-19 digital surveillance was increasingly deployed by governments around the world for tracking and notifying citizens about contact with confirmed COVID-19 patients[50] (e.g., Google and Apple API or the PEPP-PT approach[51]). This surveillance was used for enforcing mandatory self-isolation (e.g., Hong Kong),[52] automating clearance to employees in the job market,[53] allowing entry to businesses or

---

[49] *See* Brian Pfaffenberger, *Technological Dramas*, 17 SCI., TECH. & HUMAN VALUES 282, 294 (1992) (discussing the role of interpretation in the politics of technology).

[50] *See* Servick, *supra* note 4.

[51] *See* Natasha Lomas, *Europe's PEPP-PT COVID-19 Contacts Tracing Standard Push Could be Squaring up for a Fight with Apple and Google*, TECHCRUNCH (Apr. 17, 2020, 1:47 PM), https://techcrunch.com/2020/04/17/europes-pepp-pt-covid-19-contacts-tracing-standard-push-could-be-squaring-up-for-a-fight-with-apple-and-google/?guccounter=1&guce_referrer [https://perma.cc/G8NK-T8PD] (explaining the PEPP-PT approach). Part III of this Article discusses Google/Apple API.

[52] *See, e.g.*, Samuel Y.S. Wong et al., *What Can Countries Learn from Hong Kong's Response to the COVID-19 Pandemic?*, 192 CMAJ E511, E511 (2020).

[53] *See* Paresh Dave, *Tech Firms Deploy Bluetooth Chips for Coronavirus Contact Tracing in Office*, REUTERS (May 21, 2020, 7:54 AM), https://www.reuters.com/article/us-health-coronavirus-network-tracing/tech-firms-deploy-bluetooth-chips-for-coronavirus-contact-tracing-in-office-idUSKBN22X1FJ [https://perma.cc/GNK2-EXBU].

public transportation (e.g., China),[54] and predicting the likelihood of an outbreak in particular areas.[55] Common to all these measures is the collection and analysis of sensitive health, location, and proximity data at various levels of precision.

Contract tracing apps became an issue of vigorous public debate in many countries, where a key controversy concerned privacy. Contact-tracing apps made use of the mobility and accessibility of smartphones to track the spread of the pandemic. They were designed to collect and store data on locations visited or proximity to confirmed patients, or both. Accordingly, their deployment involved some obvious privacy risks.[56] Opponents were mainly concerned about state surveillance, especially when collecting location data, which arguably has a chilling effect on civil liberties.[57] Location data showing where a person has visited could be used to infer his or her associations, political stance (e.g., attendance at demonstrations or organizational events), or personal interests.[58] Civil rights advocates pushed governments to develop privacy-friendly apps to reassure the public that data on their whereabouts was not collected or shared for any purpose other than public health.[59] The concern that surveillance would be embedded in an infrastructure that might last for years after the pandemic is over prompted calls for privacy by design in CTT. Primarily, proponents argued for consent and voluntariness, transparency, data anonymization, and data

---

54 *See* Liu Daizong et al., *3 Ways China's Transport Sector Is Working to Recover from COVID-19 Lockdowns*, THECITYFIX (Apr. 30, 2020) https://thecityfix.com/blog/3-ways-chinas-transport-sector-working-recover-covid-19-lockdowns/ [https://perma.cc/G4EG-B9YT].

55 *See, e.g.*, Francesco Bellocchio et al., *Enhanced Sentinel Surveillance System for COVID-19 Outbreak Prediction in a Large European Dialysis Clinics Network*, 18 INT'L J. ENV'T RSCH. & PUB. HEALTH 1, 11 (2021).

56 *See* Kirsten Bock et al., *Data Protection Impact Assessment for the Corona App*, FORUM INFORMATIKERINNEN FÜR FRIEDEN UND GESELLSCHAFTLICHE VERANTWORTUNG (FIFF) E.V., 9 (2020), https://www.fiff.de/dsfa-corona [https://perma.cc/95AK-CEB3].

57 *See, e.g.*, Tiffany C. Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, 52 LOY. U. CHI. L. J. 767, 779 (2020).

58 *See* Mireille Hildebrandt, *Location Data, Purpose Binding and Contextual Integrity: What's the Message?*, *in* PROTECTION OF INFORMATION AND THE RIGHT TO PRIVACY-A NEW EQUILIBRIUM? 31–62 (2014).

59 *See* Tamar Sharon, *Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers*, 23 ETHICS & INFO. TECH. S45, S47 (2021).

minimization (i.e., limiting data collection to the bare minimum necessary for public health purposes).[60]

A wide variety of design solutions emerged, each employing different architectures, reflecting trade-offs between these conflicting values. Among these, Israel's CTTs offer an interesting case study. Israel was one of the first countries to move into the vaccination phase during the COVID-19 pandemic, consequently making contact tracing efforts redundant.[61] Thus, fully grasping and analyzing the local narrative became possible at an early stage. Another reason this case study is particularly interesting is that the government simultaneously applied two parallel strategies to tackle the outbreak phases of the pandemic. The case study consists of two extreme cases of technological intervention. On one hand, HaMagen ("The Shield"), a contact tracing app allegedly consisting of one of the most benevolent technological designs, reflects a regard for users' privacy (by requiring users' consent for the app installation and use), autonomy (by making installation and use voluntary), public oversight (open-source code), and data protection (distributed database as opposed to centralized database).[62] On the other hand, allegedly one of the most malevolent technological designs is the form of mass surveillance run by the least transparent governmental body, the General Security Service (GSS). This system's affordances facilitated persistent surveillance, threatening to severely violate civil rights as it was applied mandatorily and covertly, absent users' consent to the collection and storage of their information in a central database.[63]

A. Background

Tracing technologies designed to tackle the spread of the pandemic were introduced in Israel during the early days of the outbreak. Prior to that time, contact tracing was done solely by human

---

60 *See, e.g.*, Letter from Wojciech Wiewiórowski, European Data Protection Supervisor, titled EU Digital Solidarity: A call for a pan-European approach against the pandemic (Apr. 6, 2020), https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf [https://perma.cc/A9YC-NHBX].

61 *See infra* note 171.

62 *See* text accompanying footnotes 62–69.

63 *See* text accompanying footnotes 88–99.

epidemiological investigations (HEI), where investigators determined and published COVID-19 patients' last fourteen days' locations to the general public.[64] Anyone with an overlapping location in the relevant period was required to self-isolate for fourteen days.[65] Another equally important task of the HEI was to reverse-engineer a patient's route to determine their infection source.[66]

On March 9, 2020, for the first time, the HEI were helpless while facing a patient with no clear infection source.[67] At that point, it became clear that human memory is flawed and that the scale and scope of the pandemic may require a digital solution. The Ministry of Health ("MoH") initiated two parallel technological processes. First, the MoH requested the GSS's help in tracing the patient's contacts to determine an exposure location.[68] Second, the MoH initiated the development of a new app aimed at supporting human contact tracing efforts.

For the readers' convenience, we will start by unfolding the narrative of each technology separately, although both technologies are part of the same ecosystem, and their narratives are intertwined. Then, we will turn to discuss the interface between the two sociotechnical strategies.

---

64 *See* State Comptroller of Israel, The State of Israel Response to the Covid-19 Crisis: Epidemiological investigations – Special Interim Report iii, 163–77 (Oct. 2020) [hereinafter State Comptroller Epidemiological Report], https://www.mevaker.gov.il/sites/DigitalLibrary/Documents/2020/COVID-19/2020-COVID-19-104-epidemiological-investigations%20.pdf.

65 *See, e.g.*, Press Release, State of Israel Ministry of Health, Italy Patient Under Investigation (Feb. 28, 2020), https://www.health.gov.il/English/News_and_Events/Spokespersons_Messages/Pages/28022020_1.aspx [https://perma.cc/4ZSK-8KMR].

66 *See* State Comptroller Epidemiological Report, *supra* note 64.

67 The relevant patient was not abroad during or prior to the infection and had no contact with a confirmed patient. *See* Sivan Hilai, *For the First Time: A Corona Patient whose Source of Infection is Unknown was Diagnosed in Israel; Patients' Number Increased to 39*, YNET (Mar. 9, 2020), https://www.ynet.co.il/articles/0,7340,L-5691003,00.html [https://perma.cc/NE99-J4XN].

68 The GSS legal counsel approved the MoH's request. *See* State Comptroller Epidemiological Report, *supra note* 64.

B. "If you build it, will they come?": Design & Social Norms

1. The App

The first version of HaMagen 1.0 was launched on March 22, 2020.[69] The app was described by the MoH as "a national app to combat viruses," a phrase that encompasses the high hopes pinned on the technology and its future use.[70] The app's main function was to inform users that they had been exposed to a positive COVID-19 patient.

The app's architecture reflected a serious attempt to build trust in the technology and accommodate democratic values, including privacy, autonomy, transparency, and public oversight. The original version collected and stored users' location data using the mobile phone's GPS and Wi-Fi positioning capabilities.[71] An updated version, Hamagen 2, which was released four months later, also leveraged the Bluetooth capabilities (BLE) of nearby phones using the same app to collect proximity data.[72] The collected data was only stored on the user's devices for two weeks. No information was transferred from the app to government authorities or any other third party. Indeed, the government collected data on locations visited by confirmed patients through epidemiological investigation. Yet, cross referencing the location data of COVID-19 confirmed patients with the users' GPS histories took place only on the user's phone. HaMagen retrieved location and proximity data periodically, and in the case of a match with the recorded data on the users' device, the

---

69 Official Announcement, Israel Ministry of Health, The Ministry of Health Launches the "Shield" App (Mar. 22, 2020), https://www.gov.il/he/Departments/news/22032020_04 [https://perma.cc/B8HA-DXBK].

70 Raphael Kahan, *The Ministry of Health Wants to Use the "Shield" App to Fight All Future Epidemics*, CALCALIST (May 24, 2020), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwid7_ad0cb6AhUUjYkEHW0pC9gQFnoECAMQAQ&url=https%3A%2F%2Fsecure.calcalist.co.il%2Fctech%2Farticles%2F0%2C7340%2CL-3826730%2C00.html&usg=AOvVaw3KRDcGtpJuIwq6a_Cn8LBw [https://perma.cc/2XXP-QQZX].

71 *See* Michael Birnhack & Mickey Zar, *Viruses, Privacy and Technology*, ICON-S-IL BLOG (Oct. 4, 2020), https://israeliconstitutionalism.wordpress.com/2020/10/04 [https://perma.cc/QA78-WA6Q].

72 *See HaMagen FAQ*, MINISTRY OF HEALTH, https://govextra.gov.il/ministry-of-health/hamagen-app/magen-faq-he/ [https://perma.cc/YT3L-YJ4D].

app displayed the time and location of the exposure to a COVID-19 patient, instructing the individual to contact health authorities for further information (see Figure 1).

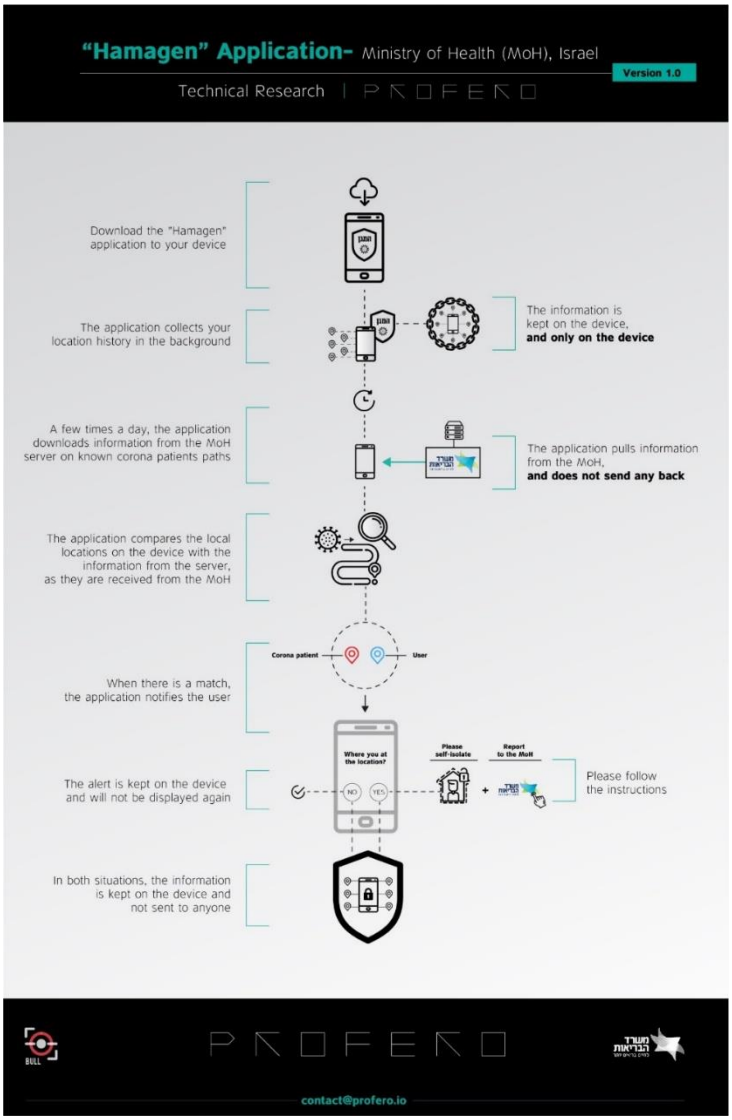

Figure 1: Hamagen (source: Israel MOH)

Another value reflected in HaMagen's architecture was a strong commitment to autonomous choice. The government collaborated with the private sector and NGOs in developing HaMagen. It

provided links to downloading the app and promoted its use in several campaigns (though this use was rather limited in scope).[73] The downloading and usage of the app were entirely voluntary, requiring users' authorization to access the tracking services on the device.[74] The app was further subject to the user's assent to the terms of use and to explicit disclosure of data collection and practices in the privacy policy.[75]

Finally, trust in the app was established through various mechanisms. A prestigious team of civil experts voluntarily consulted the MoH on various aspects of the app's design.[76] The app was later tested by several cyber and data security agencies, including Israel National Cyber Directorate, specialists from the commercial sector, and leading experts from the civil cyber and data security community in Israel. The app's design and performance were praised by professionals.[77] Moreover, the app's source code was openly published for public inspection (open source).[78] Open-source code is built on a premise of transparency in the development and deployment of software.[79] Unlike proprietary code, which is often kept

---

[73] Altshuler & Aridor-Hershkovitz, *supra* note 6.

[74] Accordingly, the terms of use open with "The State of Israel, through the Ministry of Health . . . *offer* the use of this application." *Terms of Use*, MINISTRY OF HEALTH (July 27, 2020) (emphasis added), https://govextra.gov.il/ministry-of-health/hamagen-app/ [https://perma.cc/6K2B-H2PS].

[75] *See id.*; *see also Privacy Policy and Information Security*, MINISTRY OF HEALTH (Jan. 2, 2021), https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/ [https://perma.cc/SH2J-K78U].

[76] Security checks of the open-source app included architectural checks, code reviews, and PT (breach checks). *See* Guy Bernhardt-Magen, *A Million Downloads in 4 Days: This is How the Ministry of Health's "Coronavirus App" was Developed*, GEEKTIME, (Mar. 27, 2020), https://www.geektime.co.il/hamagen-corona-app-dev/ [https://perma.cc/8MBT-HNX5].

[77] *See, e.g.*, Mikey Levy, *After the Criticism of the Mobile Surveillance: Is the "HaMagan" App Safe?*, WALLA, (Mar. 25, 2020), https://tech.walla.co.il/item/3348685 [https://perma.cc/6V29-AKCU].

[78] Ran Bar-Zik, *HaMagen's Code is Open, But There are Surprises Hidden Inside*, HAARETZ, (July 26, 2020), https://www.haaretz.co.il/captain/software/2020-07-26/ty-article/.premium/0000017f-dbd5-df9c-a17f-ffdddae40000 [https://perma.cc/TYX8-JJ42].

[79] *See also* Eben Moglen, *Anarchism Triumphant: Free Software and the Death of Copyright*, 4 FIRST MONDAY 1, 18 (1999), https://doi.org/10.5210/fm.v4i8.684 [https://perma.cc/Q63V-ZQMC]; *see generally* Maha Shaikh & Emmanuelle Vaast, *Folding and Unfolding: Balancing Openness and Transparency in Open Source Communities*, 27 INFO. SYS. RSCH. 813 (2016).

secret, open-source code is transparent and accessible, thus allowing everyone to observe its functions and providing an additional layer of trust.[80] The accessibility of the source code facilitates a traceable process which may involve open and participatory development and transparency. Potential users who distrust the government may gain access to learn what the app does or to acquire the help of those in the community to investigate the software, identify flaws, and provide solutions when necessary.[81]

All in all, the state of Israel had, from an early stage of the pandemic crisis, a state-of-the-art piece of CT technology that sought to embed fundamental democratic values. It complied with the strictest legal guidelines of the GDPR, including informed consent to proportionate data collection and effective mechanisms to ensure transparency, governmental accountability, and trust.[82]

Moreover, other general factors increased the likelihood of successful technology assimilation. Surveys suggest that in countries with a population of less than ten million and a smartphone usage rate of over 60%, CT apps had better chances of succeeding.[83] With 9.2 million residents, and a smartphone usage rate of 67%, Israeli conditions were well-suited to successful implementation of CT apps.[84] The app's assimilation prospects, therefore, seemed very promising.

---

[80] Ami Rohaks-Domba, *HaMagen Application—The Goal: To Reach Four Million Users*, ISRAELDEFENSE (June 7, 2020), https://www.israeldefense.co.il/node/43408 [https://perma.cc/E7Y4-HYSN].

[81] As was done in the case of HaMagen, see *supra* note 78 and accompanying text.

[82] *See* THE PRIVACY PROTECTION AUTHORITY, Report from July 14, 2020, http://dcx.walla.co.il/walla_news_files/06eb61b839a0cefee4967c67ccb099dc.pdf [https://perma.cc/SSR2-4NUA].

[83] *See* Privacy Israel Report, *supra* note 13 (writing that Privacy Israel surveyed 35 apps of governmental health agencies from different countries; the report was submitted to the Knesset's committee for Security and Foreign Affairs on November 29, 2020; according to the report, successful CTT apps were found in Finland, Ireland, Iceland, Singapore, Denmark, and Norway (which ceased to use the app due to privacy concerns)).

[84] *Id.* (stating that the number of smartphones in Israel is estimated at 6.2 million).

2. Assimilation & its Aftermath

At first, the app's assimilation was swift. Two days before the app was launched,[85] the first death of a COVID-19 patient was reported, followed by a general curfew which lasted several months.[86] Backed by a general atmosphere of fear, the immediate public response to the app was remarkable: a week after its launch, the app had approximately 1,000,000 downloads (even before any public campaign was set forth).[87]

The app's success, however, was temporary.[88] At its peak, out of 5.5 million smartphones in Israel, the app had 872,372 active users, which represented 17% of the MoH's target (4 million active users). That number had placed Israel sixth worldwide in CT app installments.[89] From that point, users began to uninstall it, and the MoH published a bid to upgrade it.[90] The app's update, HaMagen 2, was launched on July 27, 2020. However, by then, approximately

---

85 Ido Efrati, *First Death from the Corona Virus in Israel*, HAARETZ (Mar. 20, 2020), https://www.haaretz.co.il/health/corona/2020-03-20/ty-article/0000017f-f158-d487-abff-f3fef25e0000 [https://perma.cc/3KG8-3QA9].

86 *See* Maayan Jaffe-Hoffman & Anna Ahronheim, *Coronavirus: Infected Israelis Hit 707 as Emergency Orders Roll Out*, JERUSALEM POST (Mar. 21, 2020), https://www.jpost.com/breaking-news/529-israelis-have-been-diagnosed-with-coronavirus-health-ministry-621536 [https://perma.cc/BNR8-93ZR]. According to the orders, Israelis were not allowed to leave their homes unless it was an absolute necessity. All social interactions were prohibited, including visiting parks, beaches, pools, libraries, and museums. *Id.*

87 The MoH accompanied the launch with a minor advertising campaign, mainly on its website, which was stopped late-March/early-April, because, as the MoH's head of IT systems Rona Kaiser put it, the MoH "felt it wasn't effective enough." DK, 23rd Knesset, Session No. 17 (2020) (Isr.).

88 This was the case in some other countries, too, including the Netherlands and other EU member states. *See* Taylor, *supra* note 9, at 210.

89 *See* Presentation from MoH's Information Technologies Unit, Hamagen, to Subcommittee for Intelligence and Secret Services, 10 (May 26, 2020), https://fs.knesset.gov.il/23/Committees/23_cs_bg_572051.pdf [https://perma.cc/KF82-XCLQ]. The accuracy of these figures, however, has been disputed. *See* Altshuler & Aridor-Hershkovitz, *supra* note 6.

90 The bid was published on May 18, 2020, but postponed to June 17, 2020. Haim Ravia, *The Ministry of Health Publishes a Tender for the Further Development of HaMagen*, LAW.CO.IL. (May 19, 2020), https://www.law.co.il/news/2020/05/19/hamagen-tender/ [https://perma.cc/84QX-Y2UT].

half of the users had already deleted the app.[91] During the following months improved versions were released,[92] but in mid-October 2020 (about six months after the original launch), the government abandoned the app.[93] The MoH announced that "HaMagen did not deliver—not the desired number of users, not the desired reports on exposure nodes, and not the desired number of quarantines resulted from using the app."[94]

3. Failure Post-Mortem

Researchers suggested several reasons for the assimilation failure. Some pointed to technological problems stemming from the app's use of both location and proximity data.[95] The MoH claimed that technological malfunctions were behind the failure (namely, high consumption of battery life, a burdensome registration process for acquiring informed consent, too many notifications from the app, users' fear of entering quarantine because of using the app, and

---

[91] That is, 1,175,257 users. Within the first 24 hours after the new launch, 44,098 users downloaded the app, while 17,079 removed it. Adir Yanko, *More than 40% Remove the HaMagen 2 App*, YNET (Aug. 2, 2020), https://www.ynet.co.il/news/article/rkjMa4V11P [https://perma.cc/H3RW-EUTD]; *see also* Omer Kabir, *Experts Warn Against the Second Generation of HaMagen Application*, CALCALIST (July 28, 2020), https://www.calcalist.co.il/internet/articles/0,7340,L-3842312,00.html [https://perma.cc/UQ26-L8W7]. The MoH decided to halt the commercial marketing and campaign of the app, in order to better understand the reasons behind its failures. *See* Respondents 2-5 Response § 60, HCJ 6732/20 ACRI v. the Knesset (2021) (Isr.).

[92] Notably HaMagen 2.14, released in September 2020, which made the app compatible with Xiaomi Note, a producer of 30% of Israeli smartphones. *See* Apple Store Preview, *HaMagen 2 App*, APPLE (Mar. 22, 2020), https://apps.apple.com/us/app [https://perma.cc/RZ95-LDVR]. A week later, the chairman of the committee for Security and Foreign Affairs directed the MoH to release a new and better version of the app and relaunch the campaign within seven days. *See* DK, 23rd Knesset, Session No. 39 (2020) 35 (Isr.). This upgrade was never released.

[93] On October 12, 2020, the committee approved the requested extension of the GSS authorization while stating that the civil app was no longer considered a viable solution. In his closing statement, the committee's chairman, Zvi Hauser, said that "it can be said that Israel has abandoned the solution of HaMagen 2." Hauser added, "The new version . . . has been updated by 70,000 people and removed by 38,000 . . . According to the report we have before us, MoH practically abandoned this app, and does not invest in it any longer." DK, 23rd Knesset, Session No. 43 (2020) 34.

[94] DK, 23rd Knesset, Session No. 66 (2020) 3.

[95] *See* Privacy Israel Report, *supra* note 13 (attributing the failure to technological reasons stemming from the app's use of both location and proximity data).

privacy concerns).[96] Indeed, technological problems plagued many CTTs' operations from their beginnings. As global experts had initially warned, a fundamental flaw of CTTs that were developed and operated without adequate field trials was their vulnerability to false positive notifications, where apps falsely identified users as being exposed to an infected contact.[97] Similarly, HaMagen exhibited both technical errors resulting from inaccuracies in cellular location tracking and human errors in data entry on the MoH's servers.[98] The update's addition of BLE data to pre-existing use of GPS data turned users' attention to the need to keep Bluetooth on at all times.[99] It also exhausted battery while the app was working in the background—up to 15%—with no direct and clear benefit to the user.[100]

HaMagen also suffered from other ailments of CTTs' assimilation that were recorded in the literature: a major cross-cultural reason for CTT's assimilation failure is connected to trust in governmental authorities.[101] Thus, the technological aspect of trust, that is, trust in the efficacy of technology, is but one aspect of the issue. The social aspects of trust are no less important. At the individual level, trust is solidarity, so for an app's assimilation to be successful, individual users must trust their peers to behave in a similar manner.[102]

---

96 *See* Respondents 2-5 Response § 60, HCJ 6732/20 ACRI v. the Knesset (2021) (Isr.).

97 *See* Taylor, *supra* note 9, at 210.

98 *See* Tehilla Altshuler & Rachel Aridor-Hershkovitz, *GSS Authorization to Eradicate Corona Virus*, ISR. DEMOCRACY INST. (July 14, 2020), as Presented to the Sub-Committee for Intelligence and Secret Services, 24th Session Protocol (July 15, 2020), https://fs.knesset.gov.il/23/Committees/23_cs_bg_576597.pdf [https://perma.cc/T7FJ-2WDY].

99 *See* Sagi Cohen, *HaMagen 2 Will Not Save Us From Covid Either—and Apple and Google are to Blame for That*, MARKER (June 24, 2020), themarker.com/technation/2020-06-24/ty-article/.premium/0000017f-f4fd-d460-afff-ffffe4b20000 [https://perma.cc/A895-TKBX].

100 *See* Kaiser, *supra* note 87.

101 *See* Altshuler & Aridor-Hershkovitz, *supra* note 6. Israeli research conducted by the Israeli Democracy Institute (IDI) argued that in most countries, the low adoption rates of CT apps were attributable to lack of trust in government and their use of the personal data collected by the apps. *Id.* Besides the lack of trust, the report further attributed the Israeli implementation failure to insufficient awareness and the lack of a public campaign, as well as technical failures arising from the choice not to use the Google/Apple protocol. *Id.*

102 Lack of solidarity was a hinderance for CTTs' assimilation, with the Swiss example as a notable exception. *See* Urs Gasser, *Trust and Digital Contact Tracing: Initial Insights from the Swiss Proximity Tracing System*, MEDIUM (June 25, 2020), https://medium.com/berkman-klein-center/trust-and-digital-contact-tracing-initial-

Ultimately, the success of the CTT (which involves voluntary self-compliance) depends on a sense of duty, care, and reciprocity shared by society members.[103] Trust at the institutional level means that for an app's assimilation to be successful, individual users must trust different authorities to protect their best interests.[104] This includes trust that user data will be protected and will not be misused for other purposes, and that the system will operate in an equitable manner.[105]

Moreover, even though the app's installation and use were completely voluntary, they still involved harsh consequences, including the imposition of a self-isolation duty on those who received a notice.[106] The value associated with protecting one's social acquaintances was supposed to mitigate the risks associated with monitoring. Presumably, users would be willing to protect the health of their acquaintances at the risk of being quarantined if notified by the app. Apparently, this reasoning was not persuasive enough to build the needed level of social solidarity at the time.[107]

And so, the hopes that were pinned on HaMagen did not materialize. The desirable values embedded in the app were useless when

insights-from-the-swiss-proximity-tracing-system-53a22e20f995 [https://perma.cc/4P64-63JV].

[103] *See, e.g.*, Michael Siegrist & Alexandra Zingg, *The Role of Public Trust During Pandemics: Implications for Crisis Communication*, 19 EU PSYCH. 23, 25 (2014).

[104] *See* John Palfrey & Urs Gasser, *Planning for the Next Pandemic: A Global, Interoperable System of Contact Tracing*, 21 GEO. J. INT'L AFFS. 5, 6 (2021). Unlike the approach taken in this article, Palfrey and Gasser advocate embedding equity as a value in the design of future CTTs without considering the broader contexts of such future assimilation processes. *See id.*

[105] *Id.*

[106] *See supra* notes 87–88 and accompanying text.

[107] Psychological factors were also involved in users' decisions whether to use such technology or not. For example, aversion to bad news resulted in reluctance to use a piece of technology that is capable of bringing bad news at any moment, out of one's pocket. *See* Federica Lucivero et al., *Normative Positions Towards COVID-19 Contact-Tracing Apps: Findings from a Large-Scale Qualitative Study in Nine European Countries*, 32 CRITICAL PUB. HEALTH 5, 8–14 (2022), https://www.tandfonline.com/doi/pdf/10.1080/09581596.2021.1925634 [https://perma.cc/7ZA8-8VE6]. Also, fear of dilemmas (whether to follow the app's notification and self-isolate or to keep working based on a lack of symptoms) motivated the decision on whether to install such an app on one's device. *See id.* at 11.

facing system malfunctions, lack of social solidarity, and lack of trust in the authorities.[108]

The key actor in the struggle for technological assimilation, in this case, turned out to be the user. End-users in the contemporary digital sphere are too often portrayed as helpless infants in need of a guardian.[109] HaMagen's failure points to the contrary, demonstrating that users should be taken more seriously, as central players in the process of technological assimilation. The values-by-design approach was also supposed to overcome some well-documented obstacles to the assimilation of the app, namely, users' illiteracy and reluctance to assert their fundamental rights.[110] The HaMagen case shows, however, that end-users can reject a well-meaning piece of technological design if they are not convinced by its operators' intentions or whether it would serve their best interests.

Nonetheless, the explanation for the failure of HaMagen remains incomplete unless examined in the context of a wider ecosystem. In order to fully grasp the failure of the app, its causes, and its consequences, we need to complete the picture by examining the parallel CT technology, the GSS TOOL, and the governmental decision concerning the Google/Apple API and its ramifications for the functionality of HaMagen 2.

C. "The Fix is in": Shaping Design by Law

1. The TOOL

Since 2002, the GSS has been building a classified surveillance system known as "the TOOL," for which little public official

---

[108] *See* Altshuler & Aridor-Hershkovitz, *supra* note 6.

[109] For a recent example, see Arwa Mahdawi, *The Guardian View on Online Dangers: The Internet Needs a Retrofit*, GUARDIAN, (Apr. 26, 2022), https://www.theguardian.com/commentisfree/2022/apr/26/the-guardian-view-on-online-dangers-the-internet-needs-a-retrofit [https://perma.cc/TSS2-4GL3].

[110] *See* Matthew Paul Huenerfauth, *Design Approaches for Developing User-Interfaces Accessible to Illiterate Users* (AAAI Technical Report No. WS-02-08, 2002), https://www.researchgate.net/publication/228579579_Design_approaches_for_developing_user-interfaces_accessible_to_illiterate_users [https://perma.cc/TDG3-YYS8] (discussing the importance of such considerations).

information is available.[111] The TOOL, which was apparently designed to address threats to national security, is capable of tracking all cellular phones running in Israel through cellular communications providers.[112] As reported by the media, metadata is collected, including the device's location, the cell and antenna zone to which it is connected, callers' information (voice or text) sent or received by the cellular device, and internet browsing history.[113] The TOOL offered invasive surveillance capabilities, which posed serious threats to human rights. As analyzed below, the case study of the TOOL's assimilation during the COVID-19 crisis demonstrates how technology, which was originally designed to serve a specific purpose (national security), reflecting a given set of trade-offs, could be repurposed to serve a new task, thus changing its sociotechnical meaning without modifying the design itself. While some measures which threaten human rights might be justifiable as lesser, if inevitable, evils in the context of combatting terrorism, the use of the TOOL in a civil crisis was perceived as illegitimate from a human rights' perspective.[114]

Upon a surge in COVID-19 cases in the early days of the pandemic, the Prime Minister announced the intention to use "digital technological means" for contact tracing, and in early March 2020, the MoH urgently requested the GSS's assistance in its contact

---

[111] *See* Ronen Bergman & Ido Shwartztoch, *The Tool, the GSS Secret Database, Collects Data on Every Israeli Citizen and Knows: Where Have You Been, Who Did You Talk to, and When Did You Do All That*, YEDIOT ACHRONOT (Mar. 25, 2020), https://www.yediot.co.il/articles/0,7340,L-5701611,00.html [https://perma.cc/28RQ-G4PZ].

[112] *Id.* Section 7 of the General Security Service Law, 5762-2002, SH No. 1832 (Isr.) authorizes the GSS to receive communications data from communications companies. Chapter Four, ¶ 13 of the Communications Law (Telecommunications and Broadcasting) 5742-1982, SH No. 1059, 229, 234 (Isr.) obliges communications companies to assist the GSS and grants them immunity in this regard. Sections 4–5, 9a of The Wiretapping Law, 5739-1979, SAH No. 938 (Isr.) regulates wiretapping carried out by the GSS.

[113] *See* Eran Toch & Oshrat Ayalon, *How Mass Surveillance Can Crowd Out Installations of COVID-19 Contact Tracing Apps*, ARXIV (Oct. 4, 2021), https://arxiv.org/pdf/2110.01567.pdf [https://perma.cc/5N5K-GP9V].

[114] *See* Michael Birnhack, *Privacy in Crisis: Constitutional Engineering and Privacy Engineering*, 24 L. & GOV'T ISR. 149, at 7 (2022). Some even perceived it as a new chain in the process of securitization and militarization of the Israeli public sphere. *See* Marciano, *supra* note 15, at 85.

tracing efforts.[115] Soon enough, the head of the GSS approved a continuant assistance to the MoH on a larger scale, conditioned upon authorization by law.[116] The operation of the GSS is strictly regulated by law, with different oversight mechanisms intended to ensure compliance with the rule of law.[117] The Israeli Cabinet decided, through emergency regulations, on "Authorizing the GSS to assist in the national effort to contain the spread of the novel Coronavirus" [Decision 4897].[118] The TOOL was operated covertly, and ironically, the Israeli public became aware of its existence only in the wake of the pandemic.[119] What exacerbated the public distrust was a political crisis, prompting deep suspicion towards the repurposing of the TOOL as a civilian CTT.[120] The pandemic hit Israel in the midst of an ongoing constitutional crisis caused by an ongoing governmental instability. The government that approved the emergency powers was a transitional government headed by Prime Minister Benjamin Netanyahu, following the general elections held on March 2, 2020, and before the convention of the new parliament (the Knesset).[121] The election round was the third in a series of inconclusive

---

115 State Comptroller of Israel, The State of Israel Response to the Covid-19 Crisis: Activation of technological capabilities of the General Security Service—Special Interim Report iii, 92 (Oct. 2020) [hereinafter State Comptroller GSS Report].

116 *See id.* at 92–93.

117 *See* Amir Cahane, *Israel's SIGINT Oversight Ecosystem: COVID-19 Secret Location Tracking as a Test Case*, 19 U.N.H. L. REV. 451, 460–61 (2021). The operation of the Israeli GSS is enshrined in the General Security Service Law, 5762-2002, SH No. 1832 (Isr.) [hereinafter GSS Law]. Oversight mechanisms include a quarterly report to the Prime Minister and the AG, and a yearly report to the Knesset's Intelligence Services Subcommittee, whose deliberations are classified. *See* GSS Law §§ 6, 12. The GSS Law defines, inter alia, the powers of the organization, its subordination to the government, and the powers of overseeing its activities. *See id.* §§ 4, 7–11.

118 *See* Cahane, *supra* note 117, at 474. The decision authorized the GSS to "receive, collect and process technological data in order to aid the MoH in epidemiological investigations meant to trace the location and routes of a confirmed Covid-19 patient" for thirty days. *See* State Comptroller GSS Report, *supra* note 115.

119 That is, after the publication referenced previously in *supra* note 111.

120 *See* Niva Elkin-Koren, *Judicial Review of Digital Tracking Measures in Coronavirus Outbreak*, INTERNET POL'Y REV. (Mar. 20, 2020), https://policyreview.info/articles/news/judicial-review-digital-tracking-measures-coronavirus-outbreak/1451 [https://perma.cc/Z5HU-ZYGX].

121 General elections were held in Israel on March 2, 2020, to elect members of the 23rd Knesset. *See History*, KNESSET, https://m.knesset.gov.il/EN/About/History/Pages/KnessetHistory.aspx?kns=23 [https://perma.cc/AJF9-SG 92]. The election result showed a

rounds, which began in April 2019.[122] The transitional Cabinet pushed to approve the use of the TOOL [Decision 4897] by the Parliament Sub-Committee for Intelligence and Secret Services.[123] However, the Sub-Committee did not reach a decision because the 22nd Knesset dissolved mid-deliberations, and the Committee was disassembled.[124] Instead, the Israeli Cabinet decided, with the approval of the Attorney General (AG), to authorize the use of the TOOL, exercising its powers under emergency regulations.[125] Pursuant to Emergency Regulations, the Prime Minister holds the power to prescribe the use of technology in times of emergency.[126] Since the acting Israeli PM at the time was not re-elected after three consecutive elections, the authorization for the GSS deployment carried the flavor of a deep fear from an authoritarian regime.

The lack of legitimacy of an unelected transitional government, the absence of a functioning Parliamentary Review during the critical hours when emergency powers were exercised, and the national

political stalemate, which was ultimately resolved by way of a coalition agreement between Likud and Blue & White. *Id.*

122 Yaël Mizrahi-Arnaud & Aaron Stein, *Israel Goes to the Polls . . . Again*, FOREIGN POL'Y RSCH. INST. (Mar. 11, 2020), https://www.fpri.org/article/2020/03/israel-goes-to-the-pollsagain/ [https://perma.cc/3BEH-U6LV].

123 *See* State Comptroller GSS Report, *supra* note 115.

124 *Id.*

125 *See* Basic Law: The Government, SH 1780 (2001) 39 (Isr.) (authorizing government, during a state of emergency, to adopt emergency regulations "for the defense of the State, public security and the maintenance of supplies and essential services."). Emergency regulations may last for a period of three months unless extended by law or revoked by legislation or a decision of a majority of the members of Knesset, or if the state of emergency has ceased to exist, under conditions specified in the Basic Law. *See id.* at 39(f)–(h). Regulations were published on March 17, 2020, and expired on March 31, 2020. *See* Emergency Regulations (Authorization of the General Security Service to Assist in the National Effort to Contain the Spread of the Novel Coronavirus), 8393-2020, KT 4899, 575,782–83 [hereinafter GSS Emergency Regulations]. These regulations were replaced by two government decisions extending surveillance authorities to April 30, 2020. *See* Certification of the General Security Service to Assist in the National Effort to Reduce the Spread of the New Corona Virus and the Cancellation of a Government Decision (Resolution No. 4950) 2020, https://www.gov.il/he/departments/policies/dec4950_2020 [https://perma.cc/YW5J-U3T7]; Certification of the General Security Service to Assist in the National Effort to Reduce the Spread of the New Corona Virus (Resolution No. 4916), https://www.gov.il/he/departments/policies/dec4916_2020 [https://perma.cc/B67H-T488]. For the Israeli permanent state of emergency, see Marciano, *supra* note 15, at 86–87.

126 *See* General Security Service Law, 5762-2002, SH No. 1832 179 (Isr.).

lockdown, which caused partial closure of the courts by an administrative decree[127] had undermined the basic safeguards of the rule of law. This also deepened public distrust in the government's actions. The assumption that governmental decisions approving the involvement of the GSS could easily gain legitimacy amid a civil crisis proved to be unrealistic. Thus, the battle for authorization of the TOOL's use began.

2. The TOOL's Assimilation Battle

The assimilation process in the case of the TOOL concerns the legitimization of repurposing a pre-existing technology, namely, using an already-assimilated technology for purposes other than those for which it was originally intended. This case demonstrates how the assimilation process could reshape the technological affordances (immersive surveillance) of a given design and modify the value trade-off embedded in such design, without introducing any changes to the system itself.

The repurposing of the TOOL in the COVID-19 crisis was followed by a fierce public debate in the Israeli parliament, in the press and in academic forums.[128] Yet, the battle for authorization of the TOOL was being fought, first and foremost, in the corridors of the Israeli High Court for Justice (HCJ). The HCJ was called up to fill the gap in checks and balances caused by the exercise of emergency powers in the extreme conditions of the pandemic.[129] Human rights organizations and the HCJ have thus become central players in the battle to restrain the TOOL's operation.[130]

---

[127] The Minister of Justice of Israel at the time, Amir Ohana, issued an emergency decree of partial closure of the courts due to a national lockdown. *See* Announcement in the Official Gazette 8744 (Apr. 8, 2020); Guy Lurie, *Ministerial Emergency Powers Over Court Administration in the Israeli Judiciary*, 12 INT'L J. CT. ADMIN. 1, 8 (2021), http://doi.org/10.36745/ijca.383 [https://perma.cc/9VT6-D8YH].

[128] *See, e.g.*, Altshuler & Aridor-Hershkovitz, *supra* note 6; Rotman, *supra* note 1.

[129] *See* Birnhack, *supra note* 114, at 4–6.

[130] Decision 4897 was followed by a petition to the Israeli HCJ, filed by Advoc. Shachar Ben Meir, The Association for Civil Rights in Israel (ACRI), and The Adallah—Legal Center for Arab Minority Rights in Israel, an independent human rights organization and legal center that seeks to promote human rights in Israel in general, and rights of the Palestinian minority, with special attention to the Arab citizens of Israel (around 1.5 million people, or 20% of the population). *See* HCJ 2109/20 Shachar Ben Meir, Adv. v. Prime

The restraint of the GSS's power was a recurring process that began with public outcry, followed by legal and parliamentary review, which was backed by an impressive degree of self-restraint by civil servants, most notably the heads of the GSS.[131] The significance of self-restraint by civil servants cannot be overstated. During the relevant period, the heads of the GSS expressed an explicit reluctance to lend the organization's capabilities to the mission.[132] This explicit reluctance was characterized by the GSS and its leaders' attitude toward the demand for using the service's technological capabilities for what was perceived by them as a civil (as opposed to military) task. Publicly exposing the organization's abilities, and even worse—as became evident later—exposing its inabilities, was not welcomed by the GSS leaders. This unwillingness reached its peak in mid-June 2020 when the head of the GSS implored the Cabinet in a closed meeting not to legislate the Authorization Law and to turn instead to civil options.[133]

The assimilation of the TOOL at the legal front was marked by three major milestones: (1) an HCJ Interim order requiring parliamentary oversight (March 19, 2020);[134] (2) an HCJ decision requiring authorization by primary legislation (April 2020)[135] and subsequent legislation (July 2020);[136] and (3) the HCJ curbing the use of

---

Minister of Israel, ¶ 9 (2020) (Isr.), *translated in* VERSA: A PROJECT OF CARDOZO LAW SCHOOL, https://bit.ly/3fEhUt6 [https://perma.cc/E5HR-U7DF].

131 For the reluctance of the head of the GSS, see, for example, State Comptroller GSS Report, *supra* note 115, at 98.

132 This attitude was evident right after the first request for assistance by the MoH. Although the head of the GSS authorized the request ad-hoc, he stated that despite the ongoing "national emergency," the use of the TOOL should be limited to its "unique [original] purpose." He added that neither special resources nor employees would be allotted to the task. *See* State Comptroller Epidemiological Report, *supra* note 64, at 98.

133 Noa Landau, *Nadav Argaman Recorded at the Corona Cabinet Hearing: "GSS Surveillance Is Not the Solution"*, HAARETZ (June 21, 2020), https://www.haaretz.co.il/news/politics/2020-06-21/ty-article/0000017f-f47d-d487-abff-f7ffa8750000 [https://perma.cc/B3YF-9K35].

134 March 19 Interim Order, HCJ 2109/20 Ben Meir v. Prime Minister of Israel, ¶ 2 (2020) (Isr.).

135 *See* HCJ 2109/20 Ben Meir v. Prime Minister of Israel (2020) (Isr.).

136 Authorizing the General Security Service to Assist in the National Effort to Minimize the Spread of the New Covid Virus and Promoting the Use of Civil Contact-Tracing Technologies (Temporary) Act, 2020 [Hereinafter GSS Authorization Law].

the TOOL (March 2021).[137] We briefly discuss these milestones below to demonstrate how the affordances of the technology were shaped through the legal assimilation process.

Establishing Parliamentary Oversight. The GSS Emergency Regulations granted broad surveillance authorities to the GSS.[138] They empowered the GSS to assist the MoH in conducting epidemiological investigations by collecting and processing technological information on a patient's location and movement (limited to metadata only and excluding the content of conversations)[139] during the fourteen-day period prior to the patient's diagnosis.[140]

Several petitions were filed with the HCJ, challenging the Government's authority to authorize the use of the TOOL. The HCJ issued an interim order prohibiting the implementation of the regulations in the absence of parliamentary oversight.[141] It was held that if the Knesset did not establish the relevant committees for parliamentary oversight of the GSS emergency regulations within forty-eight hours, the GSS authorization would be nullified.[142] The hearings provided a first step in restraining the TOOL, an extensive surveillance technology, in extreme emergency conditions. First, the justices interrogated the agency representatives (in part behind closed doors) to learn more about the specific measures and procedures that were applied.[143] This was an essential step in building accountability in technology that was previously kept secret. Second, the HCJ

---

137 *See* HCJ 6732/20 ACRI v. the Knesset (2021) (Isr.).

138 The regulation empowered the GSS to assist the Ministry of Health in conducting an epidemiological investigation to reduce and prevent the spread of the novel coronavirus by authorizing the GSS to receive, collect, and process technological information. Access to this technological information allowed the GSS to perform a test pertaining to the fourteen-day period before a patient's diagnosis, to determine the patient's location and movements and identify people who came into close contact with the patient. GSS Emergency Regulations, *supra* note 125, § 2.

139 Pursuant to the regulation, the GSS may transfer to the MoH "technological information," excluding the contents of conversations as defined in the Secret Monitoring Law, 5739–1979, 33 LSI 141 (Isr.).

140 *See* GSS Emergency Regulations, *supra* note 125, § 2.

141 *See* Birnhack, *supra* note 114, at 4.

142 HCJ 2109/20 Ben Meir v. Prime Minister of Israel, ¶ 2 (2020) (Isr.).

143 Yael Fridson, *Corona HCJ: GSS Tracking is Allowed, Meantime Police is not Allowed to Enforce*, YNET, (Mar. 19, 2020), https://www.ynet.co.il/articles/0,7340,L-5698362,00.html [https://perma.cc/383P-2632].

decision triggered public oversight.[144] It pushed for the establishment of the Security and Foreign Affairs Committee by the Knesset Organizing Committee, thereby facilitating public oversight through deliberation by elected representatives and through public hearings which were broadcasted, enabling participation of civil society organizations.[145]

Restraining use by primary legislation. In a decision held on April 26, 2020, the HCJ addressed the need for governing the TOOL by primary legislation.[146] Until that point, the government had opted to use the TOOL by virtue of its powers under the GSS Authorization Law.[147] Pursuant to the law, the government had the power to authorize the GSS to engage in additional activities (other than those explicitly enumerated by the law) "in any other area determined by the Government . . . which is designed to safeguard and promote State interests vital to the national security of the State," [148] subject to the approval of the Knesset Committee on the Service Affairs.[149] The petitioners argued that the government did not have the power under the law to grant the GSS authorization in areas involving public health because the law only applies to national security threats.[150] They further argued that the massive surveillance of citizens by the GSS violated the constitutional rights to privacy and dignity and undermined the democratic system of checks and balances.[151]

The HCJ held that the government's decision to authorize the GSS passed constitutional review under the exigent circumstances

---

144 The HCJ held that GSS Emergency Regulations will remain in effect subject to oversight by the committee. HCJ 2109/20 at §§ 3–4.

145 *See* State Comptroller GSS Report, *supra* note 115, at 93.

146 *See* HCJ 2109/20 Shachar Ben Meir, Adv. v. Prime Minister of Israel, ¶ 14 (2020) (Isr.).

147 *See* Birnhack, *supra* note 114, at 3–4.

148 General Security Service Law, 5762–2002, SH No. 1832 § 7(b)(6) (Isr.).

149 Knesset Foreign Affairs and Defense Committee, and the Sub-committee for Intelligence and Secret Services of the Knesset Foreign Affairs and Defense Committee. The committee serves as the Knesset committee for the Service matters with regard to the GSS Law. The chairman of the committee is the chairman of the Foreign Affairs and Defense Committee. *See id.*

150 *See* HCJ 2109/20 Shachar Ben Meir, Adv. v. Prime Minister of Israel, ¶ 9 (2020) (Isr.).

151 *Id.* ¶ 10.

at the time it was made.[152] Importantly, however, it was held that further recourse to the GSS for the purpose of contact tracing should be set forth in primary legislation due to the severe violation of privacy.[153] Additionally, the HCJ held that such legislation should be provisional in nature and enacted as a temporary order.[154]

In July 2020, the GSS Authorization Law was enacted.[155] The law was temporary and set to expire on January 20, 2021.[156] It stipulated several requirements for the operation of the GSS amidst the pandemic: (1) the existence of an immediate and real need for GSS assistance; (2) a governmental conviction that no suitable alternative is to be found; and (3) at least 200 verified patients.[157] Pursuant to the law, the GSS authorization would be granted for twenty-one days at a time and would be subject to the continuing approval of the Foreign Affairs Committee.[158]

The GSS Authorization Law marked an important milestone in legally restraining the extended capabilities of data collection and processing enabled by the TOOL. First, the law explicitly defined the type of data that could be legally collected and processed. Authorization applied to *Technological Data*, namely, Identification Data ("Name, ID number, telephone number and date of birth"),[159] Location Data ("The location data of a cellular phone device")[160] and Call Record Data" ("Incoming call phone number, outgoing call phone number and the time of the call.").[161] Importantly, the scope

---

152 *Id.*

153 The court noted that the violation of privacy was particularly severe for two primary reasons: First, the nature of the GSS—a preventive security service which was authorized to track the State's citizens. Second, the fact that surveillance was coercive and nontransparent. *Id.* ¶¶ 38, 47.

154 *Id.* ¶ 33.

155 GSS Authorization Law, *supra* note 136.

156 *See* State Comptroller GSS Report, *supra* note 115, at 95.

157 *See* GSS Authorization Law *supra* note 155, § 3.

158 *See id.* §§ 3A, 3(d), 12A. Additionally, the law required the MoH to develop a civil CTT, and make the technology public within a week from the law's publication. *See id.* § 12A(e).

159 *Id.* § 5.

160 *Id.* § 2.

161 *Id.*

of data to be processed did not include the content of communication.[162]

The authorization to process Technological Data was limited to data pertaining to confirmed patients and individuals with whom they had been in close contact for the fourteen-day period preceding their diagnosis.[163] The law further restricted the type of data to be shared with the MoH[164] and specified certification and authorization processes for the handling of such data.[165]

Second, the law further defined rules regarding data retention (how data must be maintained and when it should be deleted).[166]

Finally, the Authorization Law established several mechanisms for oversight,[167] as well as procedures to inform individuals that their data had been processed by the GSS[168] and to allow for appeal and redress.[169]

Overall, the GSS Authorization Law sets restrictions on the close-to-infinite surveillance affordances of the TOOL. By shaping the behavior of different stakeholders who were using the technology, the law effectively shaped the social outcome of this surveillance tool. Indeed, the social harm involved in mass surveillance did not vanish. However, by explicitly defining the rights and duties of those who were operating the technology, as well as those who were subject to it, the law established a basis for contesting, challenging, and socially negotiating the scope of permissible use. Thus, the issue of design choices became an overt legal arena.

---

162 *Id.* § 2A ("Identification data, location data and Call Record data, excluding the content of a conversation as defined in the Wiretap Law, 1979.").

163 *Id.* § 5.

164 *Id.*

165 *Id.* § 14 ("Restrictions on the use of information in the service, and the certification of officials . . . ."); *id.* § 16 ("Restrictions on access to and review of information in the Ministry of Health, and certification of officials").

166 *See, e.g.*, *id.* § 13 (concerning data retention and deletion by the GSS); *id.* § 15 (concerning data retention and deletion by the MoH).

167 For instance, the GSS was required to report on a weekly basis to the Foreign Affairs and Security Committee of the Knesset and to the Attorney General's office. *See* GSS Authorization Law, *supra* note 155, § 19.

168 *Id.* § 6(c), § 8.

169 *See id.* § 8.

Curbing the use of the TOOL. Again, the GSS Authorization Law was challenged in the HCJ.[170] The petitioners argued that almost three months after the GSS surveillance was renewed, it appeared that the TOOL was ineffective and that the data showed that the GSS surveillance's contribution to the fight against COVID was very marginal.[171] If the leaders of the GSS feared that the TOOL's vulnerabilities would be publicly exposed, these data proved their fear to be reasonable.

In March 2021, nearly a year after the MoH began harnessing the GSS surveillance measures for COVID-19 location tracking, the court partially granted the petition.[172] Notably, it was decided by Chief Justice Hayut that the court hearing would be broadcasted live.[173] Accordingly, the norms set by the court regarding

---

[170] Four consecutive petitions were issued by civil rights organizations, challenging the GSS Authorization Law while the Cabinet extended the ordination of the Law. The first petition, HCJ 4762/20 ACRI v. the Knesset (2020) (Isr.), was filed ten days after the acceptance of the temporal GSS Authorization Law. By July 20, 2020, the full GSS amended law was enacted by the parliament. *See* GSS Authorization Law, *supra* note 136. The amendment entailed the dismissal of the ACRI petition, and not surprisingly, it was also followed by another petition, now challenging the amended GSS Law. *See* HCJ 5261/20 Ben Meir v. the Knesset (2020) (Isr.). This petition was dismissed on August 20, 2020. On August 16, 2020, ACRI filed HCJ 5746/20 ACRI v. the Knesset (2020) (Isr.) (an amended version of the dismissed HCJ 4762/20). This petition was also dismissed because ACRI failed to exhaust administrative remedies prior to filing the petition. *Id.* On September 24, 2020, ACRI filed the fourth petition against the law. *See* HCJ 6732/20 ACRI v. the Knesset (2021) (Isr.).

[171] The MoH's July 2020 report asserted that the percentage of verified patients among the total isolated based on the TOOL was only about 5%. *See* Ministry of Health, L. Dep't, GSS Authorization Report, Presented to the Sub-Committee for Intelligence and Secret Services (Mar. 25, 2021). The MoH's report from March 2021, however, showed that the percentage declined to 2.2%. *Id*. The State Comptroller's report from October 2020 stated that while the effectiveness of the GSS was 3.5% in the first round of operations and 4.6% in the second round of operations, the effectiveness of human investigations was 24%. *See* State Comptroller Epidemiological Report, *supra* note 64.

[172] It should be noted that when the court granted the petition, it was already announced that the state of Israel was negotiating with Pfizer regarding vaccines. On December 20, 2020, the vaccination campaign began, first with vaccinations given to medical personnel, elderly people, and people with prior conditions. *See* Isabel Kershner, *How Israel Became a World Leader in Vaccinating Against Covid-19*, N.Y. TIMES (Oct. 3, 2021), https://www.nytimes.com/2021/01/01/world/middleeast/israel-coronavirus-vaccines.html [https://perma.cc/2SA8-URAK]. The high hopes pinned on vaccination at the time may have also affected the inclination towards curbing digital surveillance.

[173] *See* Tomer Ganon, *Hayut: "It is Impossible for Us to Accept Living with the GSS's Draconian Tool Without an Alternative,"* CALCALIST (Apr. 16, 2020),

consideration of the use of state surveillance were more transparent to the Israeli public.

The court accepted the claim that the GSS Surveillance Law had seriously violated human rights, especially the right to privacy, and was not worthy of a democratic state.[174] The Court was not convinced by the governmental rhetoric as to the necessity of the TOOL's use, which leaned on the alleged conflict between a right to life and a right to privacy.[175]

The court demanded that the state develop clear regulations if the TOOL's use was to be continued and that such use be authorized in limited circumstances only.[176] The court explained that, should the state decide to extend the TOOL authorization, it will have to formulate objective criteria regarding the scope of the GSS assistance, "to put an end to the practice of using GSS assistance in a sweeping manner."[177] Writing for the majority, Justice Hayut held that the ongoing collection of location data and its transfer between public bodies without the consent of subjects and without providing any details on the type of information collected and communications included in it, was a severe violation of freedom.[178] Privacy, she held, is essentially the right to liberty, which is fundamental in any democratic regime.[179] Thus, against all odds, the HCJ restrained the TOOL's operation and sided with the civil rights organizations over the government.

By the end of March 2021, the Committee for Security and Foreign Affairs voted against the extension of GSS authorization and the government's request to authorize the GSS was finally declined.[180] The use of technology was curbed by the pushback of civil organizations, the legal system and by parliamentary oversight

---

https://www.calcalist.co.il/local/articles/0,7340,L-3808451,00.html [https://perma.cc/XZ5P-57C7].

174 HCJ 6732/20 ACRI v. the Knesset, § 49 (2020) (Isr.).

175 For a detailed analysis of the judges' attitudes concerning privacy, see Birnhack, *supra* note 114.

176 *See* HCJ 6732/20 ACRI v. the Knesset, §48 (2020) (Isr.).

177 *Id.*

178 *Id.* §19.

179 *Id.*

180 DK, 23rd Knesset, Session No. 81 (2021) 27 (Isr.).

mechanisms. Thus, the grave concerns regarding the use of the GSS in a civil crisis and the fear that such use will mark "the end of democracy" did not materialize due to the traditional checks and balances of the liberal democratic model, in the form of judicial and parliamentary review. In the case of the TOOL's assimilation battle, the main actors were the civil society organizations and the judicial system, representing and protecting the citizen, which was perceived as a forced user.[181]

All in all, the process of curbing the GSS's power demonstrated a rapidly growing restraint, starting with a vocal public protest, backed by civil servants, followed by legal review and parliamentary review.

D. Technological Ecosystem

To fully grasp the processes that led to the unintended consequences of the Israeli CTT strategy, it is insufficient to examine each technical solution as a separate, independent unit of inquiry. Rather this strategy must be considered in the context of a complex ecosystem that is an intricate combination of legal, social, political, and technological interfaces. As became repeatedly evident, the plots of the TOOL and of HaMagen were intertwined.

One aspect of the interface between the opposing technologies manifested in the discourse that surrounded the assimilation efforts. The Israeli government in general, and the MoH in particular, advertised their own products, HaMagen and the TOOL, in an ambivalent manner. That is no surprise because the MoH had two competing systems at hand; eventually, it was unable to promote either adequately. Immediately after its launch, HaMagen was presented as an equivalent to the GSS system in terms of functionality and

---

[181] Facing the Omicron variant, Israel again deployed the GSS TOOL for contact tracing; this time the whole process—emergency orders, a petition to the HCJ, and a decision which in fact authorized in retrospect the government decision, which in turn already expired—took only five days. *See generally* Michael D. Birnhack, *The Temporal Dimension of Surveillance*, SURVEILLANCE & SOC'Y (forthcoming 2023), https://ssrn.com/abstract=4269468 [https://perma.cc/223V-D5FR] (providing a detailed narrative and analysis of the GSS TOOL and the Omicron variant).

goals.[182] When it became apparent that HaMagen was problematic in terms of its efficiency, the MoH had to change the discourse around it.[183] Therefore, the parliamentary deliberations mainly focused on whether the app offered a suitable alternative to the TOOL.[184] Gradually, the app was portrayed as an inferior solution.[185]

The battle surrounding the legality and legitimacy of the GSS deployment in the pandemic context critically affected the governmental attitude toward HaMagen. Since the MoH wanted to obtain legal approval for the use of the TOOL, it had to deal with the following question: If the two technologies do the same thing, why do we even need the GSS, which is evidently more problematic in terms of human rights? Since the Ministry did not want to give up the more efficient GSS assistance, it was forced to claim that the GSS system and the civil app were not doing the same thing and that the TOOL had superiority over the app the Ministry itself had developed. Absurdly enough, when the HCJ ordered the government to develop a civilian substitute for the GSS, the government declared that it would do so, creating the appearance that HaMagen, which at the

---

[182] Two days after the app's launch, the HCJ ordered the GSS Emergency Regulations to remain in effect for the time being. The court stated explicitly that the special Sub-Committee for Intelligence and Secret Services, while deliberating the approval of the emergency regulations, should take into account the newly launched civilian app and decide whether the GSS TOOL is still needed. *See* HCJ 2109/20 Shachar Ben Meir v. Prime Minister of Israel (2020) (Isr.).

[183] *See, e.g.*, DK, 23rd Knesset, Session No. 10 (2020) (Isr.).

[184] During the deliberations of the Sub-Committee for Intelligence and Secret Services regarding the extension of the GSS authorization post HCJ ruling, the app was still considered as a parallel civil alternative to the TOOL. Among the background material before the committee was a memo by the Privacy Protection Authority, a statutory organ of the Ministry of Justice. According to the memo, the use of the GSS should be stopped, and more voluntary measures should be considered. The Authority Memo described HaMagen as a proper substitution for the TOOL. *See* DK, 23rd Knesset, Session No. 8 (2020) (Isr.).

[185] *See* DK, 23rd Knesset, Session No. 10 (2020) 6–8 (Isr.). Until the launch of the app's upgrade, the devaluation of the app when compared with the TOOL continued. For example, on June 23, 2020, two days after the head of GSS openly opposed the legislation of the GSS Authorization Law, a special session of the Sub-Committee for Intelligence and Secret Services was held, aimed, again, at discussing civil alternatives to the GSS surveillance. MK Orna Barbivay marked that the starting point of the discussion was that the GSS TOOL was the most effective solution, and that HaMagen is just a supplementary (and even redundant) app. *See* DK, 23rd Knesset, Session No. 17 (2020) (Isr.).

time was already deployed, was not that substitute.[186] It seems that acknowledging HaMagen's existence was perceived as something that might compromise the possibility of using the TOOL.

The government had to reframe the discourse, gradually claiming that the two solutions were not parallel and that one was superior, until finally admitting that the civil app was no longer considered a solution at all.[187] However, if that was the whole story, we would expect the TOOL to gain the upper hand. However, as was already described, that was not how things turned out.

Another interface between the technologies, which critically shaped their assimilation, was users' attitudes. The governmental policy of simultaneously employing two technological solutions affected the public attitude towards both. Indeed, four days after HaMagen was launched, experts already cautioned that the app's assimilation would fail as long as the government was using the TOOL. Civil society representatives warned during the parliamentary deliberations that the public would not use a voluntary app because they were intimidated by the GSS and were concerned about governmental mass surveillance.[188] A recent study shows that one of the main reasons HaMagen failed was the simultaneous activation of the TOOL.[189] One explanation provided by the literature is that the voluntary appeal of HaMagen appeared to be no more than an illusion of voluntariness, because the Israeli citizenry became aware that their data was collected by the GSS anyway.[190] Accordingly,

---

186 Another example of the absurdity came when the Security and Foreign Affairs Committee started deliberating on the full GSS Authorization Law, and one of the major suggested amendments proposed requiring the government to develop civil CCT alternatives to the GSS. At that time, HaMagen was already active four months. *See* DK, 23rd Knesset, Session No. 19 (2020) (Isr.).

187 *See* HCJ 6732/20 ACRI v. the Knesset, § 8 (2021) (Isr.).

188 *See* DK, 23rd Knesset, Session No. 1 (2020) (Isr.). The mentioned representatives were Prof. Hagai Levine (Chairman of the Israeli Association of Public Health Physicians) and Prof. Michael Birnhack, (privacy-law leading expert), both warning that people will not use the MoH voluntary civilian app because the GSS story intimidates them and the fear of mass surveillance is stronger than the fear of the disease. Later the President of ISOC-IL, Prof. Karin Nahon, argued that "if the GSS will monitor civilians, no one will download HaMagen." *See* DK, 23rd Knesset, Session No. 24 (2020) (Isr.).

189 Altshuler & Aridor-Hershkovitz, *supra* note 98.

190 *See* Toch & Ayalon, *supra* note 113, at 7.

the use of the TOOL lowered the public trust in the governments' intentions to protect civil rights.

Despite being a benevolent app in terms of users' rights protection, HaMagen was a part of an ecosystem that was saturated with surveillance, if only due to the TOOL's operation on every device in the country, whether it had the civil app installed or not. Moreover, it seems that HaMagen's ability to provide users such vast civil rights protection was dependent, at least in part, on the fact that the GSS provided the MoH with their data.[191] The TOOL was a reliable backup that enabled the development of a voluntary system because the MoH was never truly dependent on HaMagen's data alone.[192] This is pertinent for two reasons. One reason is voluntariness, which is desirable from a civil rights perspective, but at the same time costly in terms of efficacy, as a threshold of 60% uptake rates of contact tracing apps was required to achieve an adequate outcome.[193] In other words, voluntariness diminishes the digital system's effectiveness.[194] The second reason is that it helps us understand that the ministry's ambivalence stemmed from a problem of competing needs—users' autonomy (voluntariness) and efficacy—and that each of these needs is a stick in the other's wheels.

As a mandatory measure, the TOOL was probably superior to any voluntary app in achieving its epidemiological goals. Moreover, it appears that such technology can overcome the digital divide by applying standard surveillance to all segments of the population, regardless of class. In Israel, for instance, about 33% of the population does not own a smart device and therefore is unable to benefit from the voluntary civil app. Not surprisingly, there is a correlation

---

191 Burmeister et al., *Toward Architecture-Driven Interdisciplinary Research: Learnings from a Case Study of COVID-19 Contact Tracing Apps*, COMP. SCI. L. 143, 143–54 (2022), https://doi.org/10.1145/3511265.3550451 [https://perma.cc/G8TS-3UAU].

192 *Id.*

193 *See* Robert Hinch et al., *Effective Configurations of a Digital Contact Tracing App: A Report to NHSX* (Apr. 16, 2020), https://www.semanticscholar.org/paper/Effective-Configurations-of-a-Digital-Contact-App%3A-Hinch-Probert/1c1adf321f56da38cab0826a29812b696471ed0b [https://perma.cc/6RS4-K7ZV].

194 Mickey Zar & Michael Birnhack, *Privacy in Crisis: Privacy Guidelines for the Design of Contact Tracing Technologies*, 30 (2020), https://ssrn.com/abstract=3683166 [https://perma.cc/8MS2-EAFL].

between this population and the unprivileged and the poor.[195] The local digital divide cuts not only between the poor and the rich but also between religious and secular, as a major part of the ultra-Orthodox society owns kosher mobile devices that do not allow internet browsing.[196] A salient advantage of the GSS system was its ability to bypass this difficulty by tracing people regardless of the type of cellular device they used, since it is capable of tracing dumbphones as well. Thus, the TOOL promotes equality in a manner that contradicts its predatory aura. In this special context of public health, it might be the case that equal surveillance is better than discriminatory surveillance. Had the MoH communicated this nuance clearly, the prospects of both digital endeavors might have looked brighter.

The analysis so far has demonstrated that if we fail to take into account the broader contexts of technological assimilation, we may end up facing various unintended outcomes. We might end up with a great piece of technology, such as HaMagen, that no one wishes to adopt; we might also fail to use some competent technology, such as the TOOL, because we underestimate the power of institutional restraints; or we might end up with a private commercial technology that could lead to other unintended consequences, to which we turn next.

III. "IF YOU FAKE IT, WILL THEY COME?": SHAPING DESIGN BY THE MARKET

Zooming out to the global level, the pandemic triggered many governments around the world to introduce different types of tracing apps in an attempt to mitigate the swift spread of COVID-19.[197] The

---

[195] For a discussion on the strong correlation between populations that have no smartphones and a high mortality rate from Covid, see JEFFREY P. KAHN, JOHNS HOPKINS PROJECT ON ETHICS & GOV. OF DIGIT. CONTACT, DIGITAL CONTACT TRACING FOR PANDEMIC RESPONSE 69 (2020).

[196] Omri Levy, *A Kosher Cell Phone: The Story of the Phone for the Ultra-Orthodox*, YNET (Jan. 6, 2009), https://www.ynet.co.il/articles/0,7340,L-3650344,00.html [https://perma.cc/T5MW-9SPF].

[197] Christopher S. Yoo & Apratim Vidyarthi, *Privacy in the Age of Contact Tracing: An Analysis of Contact Tracing Apps in Different Statutory and Disease Frameworks*, 5 U. PA. J.L. INNOVATION 103, 110 (2021).

use of these measures triggered a vivid public debate over the appropriate balance between public health necessities and fundamental rights, especially in the context of privacy and data protection.[198]

Amidst these heated debates, when Google and Apple announced their "privacy preserving" API ("GAEN") for contact tracing, they were praised as privacy saviours.[199] Google and Apple comprise a duopoly which dominates the worldwide market of Mobile Operating Systems.[200] In April 2020, the two digital giants announced "a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design."[201] The GAEN API launched in May 2020,[202] answering an urgent need for interoperability between the two major operating systems: Apple's iOS and Google's Android.[203] The design specifications of GAEN incorporated some key requirements spelled out by privacy advocates.[204] The GAEN API supported Bluetooth-based apps, which enabled the collection of proximity data only.[205] Mobile phones on which CTTs were installed generated random numerical IDs ("handshakes") which were transmitted to nearby devices

---

198 *See* Lawrence O. Gostin & James G. Hodge, *US Emergency Legal Responses to Novel Coronavirus: Balancing Public Health and Civil Liberties*, 323 JAMA 1131, 1131 (2020); Rob Kitchin, *Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19*, 24 SPACE POLITY, 362, 362–81 (2020).

199 *See* Sharon, *supra* note 59, at 546.

200 *See Mobile Operating System Market Share Worldwide*, STATCOUNTER, https://gs.statcounter.com/os-market-share/mobile/worldwide [https://perma.cc/2XRM-EN4K].

201 *Apple and Google Partner on COVID-19 Contact Tracing Technology*, APPLE (Apr. 10, 2020), https://www.apple.com/il/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ [https://perma.cc/ZH2S-N2PL].

202 The Exposure Notification Framework (ENF), was later named the Google-Apple Exposure Notification Framework (GAEN).

203 *See* Mark Scott et al., *How Google and Apple Outflanked Governments in the Race to Build Coronavirus Apps*, POLITICO (May 15, 2020), https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/ [https://perma.cc/GPG9-SYCW].

204 *See* Sharon, *supra* note 59, at 546.

205 *See* Andy Greenberg, *How Apple and Google Are Enabling Covid-19 Contact-Tracing*, WIRED (Apr. 10, 2020), https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/ [https://perma.cc/RUM2-BKGM].

and stored on their history logs.[206] When a confirmed patient activated the alert system, a notification was sent to the devices whose identifiers it had previously received.[207] No personally identifiable data or location data was required.[208] Additionally, GAEN facilitated a decentralized proximity design, where all data was stored locally on each mobile device and each app could automatically initiate contact matching by itself, without having to rely on any centralized dataset run by the authorities.[209] Participation was entirely voluntary, as no information was collected on any mobile phone unless the user opted to download an app and activate it.[210] For all these reasons, the GAEN design was praised by many as privacy-preserving.[211] The joint venture of two of the world's most powerful data corporations was portrayed as a benevolent act of corporate social responsibility seeking to promote privacy for the global public's good. Ironically, Google and Apple, which are often subject to harsh criticism over their invasive data practices,[212] were suddenly portrayed as privacy champions.[213] The global hope that the corporate technology was the longed-for solution was almost as great as the corporations that devised the solution.

It was somewhat naïve, however, to assume that interoperability and a privacy-preserving design would come at no cost. Apple and

---

206 *Id.*

207 *Id.*

208 *Id.*

209 *Id.* Decentralized privacy-preserving proximity tracing was endorsed by the European Parliament (2020), and many European countries, including Germany, Austria, Estonia, and Switzerland, adopted it.

210 *Id.*

211 *See, e.g.*, Zack Whittaker, *Hundreds of Academics Back Privacy-friendly Coronavirus Contact Tracing Apps*, TECHCRUNCH (Apr. 20, 2020 9:00 AM), https://techcrunch.com/2020/04/20/academics-contact-tracing/; Commission Recommendation (EU) 2020/518 of 8 April 2020 on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data, 2020 O.J. (L 114/7) (explaining the recommendations of the European Commission "on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis.").

212 *See* Monique Mann et al., *Between Surveillance and Technological Solutionism: A Critique of Privacy-Preserving Apps for COVID-19 Contact-Tracing*, NEW MEDIA SOC'Y 1, 7 (2022) (Austl.); *see e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 238 (2019).

213 *See* Sharon, *supra* note 59, at S46.

Google restricted access to the GAEN to public health authorities and scrutinized GAEN-enabled apps against a set of criteria which, among other things, forbade the collection of location data.[214] Such data was instrumental to public health authorities in identifying hotspots of outbreak, predicting risks, and gaining a better understanding of the pandemic forecast and risks based on context-rich data. Location data was also essential in cases where the mobile phone penetration rate was low, thus requiring public health authorities to issue public warnings regarding locations where infection risk was high.[215]

States that insisted on collecting such data were prevented from using the GAEN API.[216] In that manner, the corporate endeavor collided with national efforts. This corporate strategy triggered resentment among public authorities. For instance, Cedric O, France's digital minister, criticized the two corporations for refusing to work with the French app, explaining that the French "don't want to be constrained by the internal policy choices of any company on a matter of public health."[217] In Ireland, the government shifted to the GAEN API after initially aiming at creating a centralized app.[218] A local privacy expert lamented, "we are reliant on a duopoly of tech companies that control the operating system market."[219] Similar concerns were raised by several states in the United States, including North Dakota.[220]

The GAEN initiative, which presumably ensured privacy by-design, also shaped the ecosystem, introducing detrimental implications for civil rights.

---

214 *See* Katie Hogan et al., *Contact Tracing Apps: Lessons Learned on Privacy, Autonomy, and the Need for Detailed and Thoughtful Implementation*, 9 JMIR MED. INFORMATICS 1, 9 (2021).

215 *Id*. at 4.

216 *See* Shannon Bond, *Apple, Google Coronavirus Tool Won't Track Your Location. That Worries Some States*, NPR (May 13, 2020), https://www.npr.org/2020/05/13/855064165/apple-google-coronavirus-tech-wont-track-your-location-that-worries-some-states/. [https://perma.cc/5C48-N7XV].

217 *See* Scott, *supra* note 203.

218 *Id.*

219 *Id.*

220 *See* Bond, *supra* note 214.

First, the GAEN endeavor, despite its privacy-preserving image, turned out to carry its own non-negligible privacy issues. Studies have shown that GAEN-enabled Bluetooth-based apps also facilitate "location-tracking through the use of beacons—small wireless transmitters that communicate via Bluetooth with other Bluetooth-equipped devices like smartphones, and from which granular location can be inferred."[221]

Moreover, critics claimed that a technology that is pushed into the operating system level (as opposed to the application level) is more invasive because it renders contact tracing no longer limited in time or in purpose, two important safeguards to protect privacy.[222] Also, despite the API being decentralized, the app that uses it could be centralized, thus cancelling the pro-privacy advantage.[223] The concerns became graver on September 1, 2020, when Google and Apple declared that their future smartphones would be equipped with a privacy-protective contact tracing feature.[224] The GAEN system threatened severe consequences—"the game changes because it is no longer a single app that we choose to install: it's a technology embedded in all future smartphones."[225]

Second, depriving governments of location data strengthened the dependency of governments on digital platforms in performing their duty to promote public health.[226] In fact, it undermined governmental initiatives to develop alternative, potentially privacy-preserving contact tracing apps that might have reflected a different trade-off between individual privacy rights and public health.[227] Governments that rejected the corporate solution faced

---

221 *See* Mann, *supra* note 210, at 7.

222 *See* Jaap-Henk Hoepman, *Stop the Apple and Google Contact Tracing Platform. (Or Be Ready to Ditch Your Smartphone.)*, (Apr. 11, 2020), https://blog.xot.nl/2020/04/11/stop-the-apple-and-google-contact-tracing-platform-or-be-ready-to-ditch-your-smartphone/ [https://perma.cc/DBX5-JVDK].

223 *See id.*

224 *See* Freed Benjamin, *Apple, Google: Contact Tracing to Become Standard Smartphone Feature*, STATESCOOP (Sept. 1, 2020), https://statescoop.com/apple-google-contact-tracing-exposure-notifications-express [https://perma.cc /WLX4-A6MX].

225 *See* Hoepman, *supra* note 220, at 2; *see generally* Lemos, *supra* note 2, at 97 (critiquing similar implications).

226 *See* Sharon, *supra* note 59, at S47; *see also* HELBERGER ET AL., *supra* note 5, at 17.

227 *See* Hogan, *supra* note 212, at 9; *see also* Sharon, *supra* note 59, at S54; Mann, *supra* note 210, at 8–9.

technological difficulties that were detrimental to the success of local apps.[228] Thus, even privacy-preserving apps, such as HaMagen, were forced to create workarounds,[229] which were battery-draining.[230] Studies have shown that an important reason for uninstallations of HaMagen was concern about battery consumption.[231]

Importantly, the prohibition on collecting location data further strengthened the power of the Google/Apple duopoly, which already dominates the location data market, because it prevented potential competitors, including both governmental and private actors, from collecting location data. Location data is constantly harvested from smartphones by Apple and Google.[232] The companies can also combine location data with other types of data collected from other channels to generate powerful analytics.[233] This has raised concerns over the rising power of tech giants in handling sensitive health data.[234] Moreover, the GAEN restriction on the collection of geolocation data had some dynamic implications for innovation and competition. It weakened competitive pressures and undermined prospects of developing alternative privacy preserving designs by competing market players.[235]

Finally, the GAEN example demonstrates one of the fundamental risks involved in a by-design policy approach, namely, the delegation of norm-setting power to market players.

---

228 *See* Mann, *supra* note 210, at 8–9; *see also*, Hogan, *supra* note 212, at 9.

229 *See* Hogan, *supra* note 212, at 9. *But see* Altshuler & Aridor-Heshkovitz, *supra* note 6 (arguing that Israel is not willing to use the GAEN protocol because the government is not willing to give up its centralized control).

230 *See* Hogan, *supra* note 212, at 9. On November 30, 2021, the GAEN alternative was presented before the Israeli parliament committee for Security and Foreign Affairs by Google representatives. *See* DK, 23rd Knesset, Session No. 66 (2020) (Isr.) (rejecting the corporate solution, which for HaMagen, meant technical instability and battery loss).

231 *See* Toch & Ayalon, *supra* note 113, at 5.

232 *See generally* Alfred Ng & Jon Keegan, *Who is Policing the Location Data Industry?*, MARKUP (Feb. 24, 2022), https://themarkup.org/the-breakdown/2022/02/24/who-is-policing-the-location-data-industry [https://perma.cc/CTC4 -WTZ2].

233 *See generally* Mehul Reuben Das, *Google, Apple, Meta, Amazon, Twitter: New Report Reveals Who Collects the Most Data from Users*, TECH2 (Aug. 25, 2022), https://www.firstpost.com/tech/news-analysis/google-apple-meta-amazon-twitter-new-report-reveals-who-collects-most-data-from-users-11113021.html [https://perma.cc/7JH5-P6N Q].

234 *See* Sharon, *supra* note 59, at S46.

235 *See id.* at S54; *see also* Mann, *supra* note 210, at 8–9.

By-design policy often creates a power-play between sovereign states and tech companies. While a civil rights perspective often focuses on the protection of citizens against the misuse of governmental power, there is also a growing concern regarding the potential threat to civil liberties raised by the world's big data corporations.[236]

By-design policy is often executed by tech companies. It is embedded in the design choices made by those who develop and deploy the system. As argued above, Google and Apple's decision to adopt a particular decentralized model and set limits on certain uses of data by public health authorities reflected a certain trade-off between different values, such as public health, privacy, security, competition, and innovation. Once governments opted to comply with GAEN restrictions, they basically handed over authorities and powers reserved to sovereign states.

Governmental actions are often subject to constitutional scrutiny aimed at safeguarding users' civil rights. Multinational data giants, much like governments, control powerful surveillance capabilities with much less public leverage to demand accountability.[237] The duopoly of Google and Apple in the mobile operating systems market and their power to leverage other digital services and shape global digital infrastructure[238] suggest that some check on power must be retained. Moreover, a by-design policy, where a government hands over value choices to private actors, may enable governments to bypass some legal restraints that would otherwise apply to governmental authorities.[239]

---

[236] *See* Niva Elkin-Koren, *The New Synergy: Governmental Enforcement of Speech via Digital Platforms*, *in* CONSTITUTIONALIZING SOCIAL MEDIA 180 (Edoardo Celeste et al. eds., 2022) (Isr.).

[237] Arguably, the TOOL offered a mandatory public alternative, already ready to use at the moment of crisis. Moreover, apparently the use of the TOOL in the context of the pandemic was at least partially subject to effective legal oversight, which could be seen as the lesser evil when compared to the scenario in which global data corporation gets access to the same data. *See supra* notes 128–83 and accompanying text.

[238] *See* Mann, *supra* note 210, at 11; *see also* JOSE VAN DIJCK ET AL., THE PLATFORM SOCIETY: PUBLIC VALUES IN A CONNECTIVE WORLD 4 (2018).

[239] *See* Elkin-Koren, *supra* note 234, at 183.

CONCLUSIONS: RECALCULATING ROUTES FOR HOPE

This article has attempted to draw some lessons from the case study of CTTs used during the COVID-19 pandemic. It demonstrated the limits of a by-design regulatory approach for proactively promoting policy goals by focusing solely on design decisions. It highlighted the need to consider additional forces which shape the social outcome of any given design.

The fact that the Israeli government simultaneously promoted two technologies offers a rich laboratory for studying a complex surveillance ecosystem and the co-influence of competing technological strategies. The CTTs' narrative unfolded two levels of the politics of law and technology. At the technology level, it shows that even when values and rights are embedded in technology, assimilation efforts might fail in the absence of users' active will to adopt it. Here, law plays a central role in dictating, in advance, the system specifications that would comply with legal expectations. Defining legal rights and duties and designing systems that meet these legal requirements seems insufficient when facing unconvinced users.

At another level, involving the dialectic tension between efforts to assimilate a certain technology and those which oppose it, law becomes even more central as an arbitrator in favor or against technological assimilation.

The CTT case study demonstrates both roles of the law in shaping technological affordances. On one hand, the benevolent technology that was shaped to neatly fit the legal requirements was eventually useless. On the other hand, the forces that opposed the malevolent technology managed to mobilize the legal system toward banning its use. The odd result of the ecosystem being saturated with surveillance technologies was zero technology.

The Google/Apple API suggests that technological affordances are shaped not only by social norms (as demonstrated by the assimilation failure of HaMagen) nor by the law alone (as demonstrated by the legal restraint of the TOOL). The by-design policy is often applied by market actors and shaped by market forces. As the GAEN example demonstrated, the introduction of corporate restraints by Google and Apple generated a power-play between the duopoly of digital corporations and the sovereign state, forcing the governments

who sought to collect location data to bypass GAEN API, thereby rendering the CTT less useful due to battery drainage. Overall, the unintended consequences of the alleged privacy preserving design of GAEN were the strengthening of the already dominant position of the data corporations to the detriment of civil liberties.

The CTT case study reminds us that the meaning of technology is not determined solely by pre-embedded values.[240] Additionally, the social outcome of technology is not the result of ex-ante affordances only. Rather, it is shaped by ex-post ongoing interpretation by social institutions such as the law and the market. This understanding calls for a sociotechnical ecosystem perspective, which takes into account the codependency of different social regulators. Interactions within this ecosystem are dynamic. Therefore, outcomes cannot be fully predictable.

This does not mean that engineers do not bear any ethical responsibility to the human rights implications of the systems they design. It also does not follow that governments and organizations are exempted from considering the value implications of their choice to deploy any particular design. Yet, our case study has demonstrated that social implications may depend on multiple factors. Addressing them via policy may require simultaneous effort at additional fronts: law, markets, and social norms.

There are several implications for policymakers that can be derived from recognizing the endogenous nature of technology. First, the by-design, ex-ante approach should be taken with a grain of salt, meaning that technology requires dynamic intervention strategies. Second, these interventions require the collaborative efforts of social scientists, lawyers, and computer scientists.

More generally, we are reminded that modesty is required on the part of those who think that technological design alone will provide a solution to dilemmas concerning values. On the optimistic side, it

---

[240] Indeed, in another context of Internet standard setting and protocol development, Milton Mueller and Farzaneh Badiei have recently demonstrated that it is impossible to know in advance exactly how standards will affect human rights. *See* Milton L. Mueller & Farzaneh Badiei, *Requiem for a Dream: On Advancing Human Rights via Internet Architecture*, 11 POL'Y & INTERNET 61, 74–75 (2019).

appears that it takes more than a predatory technology to undermine democracy.