On Comments Submitted to the FTC ANPR on Commercial Surveillance and Lax Data Security Practices

By Ido Sivan-Sevilla (University of Maryland), Helen Nissenbaum (Cornell Tech) and Patrick Parham (University of Maryland)

On On Comments Submitted to the FTC ANPR on Commercial Surveillance and Lax Data Security Practices

By Ido Sivan-Sevilla (University of Maryland), Helen Nissenbaum (Cornell Tech) and Patrick Parham (University of Maryland)

Introduction & Overview: Toward a Positive Definition of Privacy[1]

These comments, respectfully submitted in response to the Federal Trade Commission's (FTC) advanced notice of proposed rulemaking (ANPR) on the prevalence of commercial surveillance and data security practices that harm consumers, are based on selected research findings – our own and others. They are organized into four Parts. Part I drives a stake through the heart of direct-to-consumer consent-based approaches, arguing that notice and consent, transparency and choice, and privacy policies are not only ineffective; they may constitute "unfair and deceptive" practices. Part II addresses questions about data minimization, purpose limitations and sectoral approaches, vulnerable populations, and costs and benefits by drawing on the theory of privacy as contextual integrity (CI) (Nissenbaum, 2009). Part III discusses questions on the role of third party intermediaries in the enforcement process and facilitation of new disclosure rules, mechanisms to require/incentivize companies to be forthcoming about their data practices, and the role of civil rights agencies. Part IV suggests an adaptive regulatory model for the FTC through three regulatory learning cycles that can help the Commission account for changes in business models of surveillance-based industries.

With these comments, we urge the FTC to adopt a positive conception of privacy as its basis for the design and enforcement of new commercial surveillance rules. By focusing almost completely on privacy's role as a shield against pecuniary and psychological harms to consumers (Q.9 of the

[1] The authors thank Stephen Chan, Sydney Cohen, James Palano, and Bartley Tablante for their research assistance.

FTC), we have chronically undervalued the positive functions of privacy, understood as "*appropriate* flow of information." The positive functioning of privacy values the interests of individual data subjects, but it extends beyond them. Privacy serves societal ends by supporting and promoting societal values (e.g., fairness, autonomy, trust, liberty) as well as contextual functions, purposes, and values (e.g., healthcare, trust, learning, creativity).[2]

Privacy should be protected because of what it enables and promotes. Instead of narrowly addressing privacy as a constraining factor on commercial surveillance, we should consider the opportunity costs of inadequate protection. As a key component of social relationships, privacy builds and maintains the relations between citizens and governments (Biddle et al., 2021), consumers and corporations (Berjon, 2021), migrants and law enforcement authorities (Privacy International, 2022), as well as the interactions among peers (Zhang et al., 2022). When privacy is portrayed as antithetical to commercial benefits, efficiency, and user comfort,[3] it disserves the positive outcomes that privacy supports. System design and enforcement rules must maintain this positive view of privacy or risk losing a significant rationale for its forceful protection.

The following discusses potential guidelines for the design, monitoring, and adoption of consumer surveillance rules. Each section begins with the relevant overarching question(s) posed by the FTC for this call. During our statement, we cite the more specific FTC questions that our paragraphs address.

About the Authors

Ido Sivan-Sevilla, Helen Nissenbaum, and Patrick Parham are researchers focusing on the impact of technology and data usage on social welfare, with special attention to privacy harms and benefits, and governance structures.

[2] Helen Nissenbaum. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, USA, pg. 74. (citing Gavison, R. 1980. Privacy and the Limits of the Law. *Yale Law Journal* 89: 421-471. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, ed. F. D. Schoeman. Cambridge: Cambridge University Press, 1984, 346-402.), pg. 81 (citing Von Staden, H. 1996. In a Pure and Holy Way: Personal and Professional Conduct in the Hippocratic Oath. *Journal of the History of Medicine and Allied Sciences* 51(4): 404-437.)

[3] See Choi et al., 2020, for example, on how privacy negatively impacts profitability of advertisers and publishers.

Ido Sivan-Sevilla [homepage] is an Assistant Professor of information science at the University of Maryland. He measures and theorizes about the way our information society is governed, studying how the race between policy and technology challenges policy design and policy implementation, impacting core societal values such as security, privacy, and accountability. Ido was previously a postdoctoral fellow at Cornell Tech, a Fulbright Scholar during his MA in Public Policy at the University of Minnesota, and completed his BA with honors in Computer Science from the Technion - Israel's Institute of Technology. He has a vast network and information security background, serving at Israel's Prime Minister's Office and the Israeli Air Force [Captain].

Helen Nissenbaum is a Professor of Information Science and the Director of the Digital Life Initiative at Cornell Tech in New York City. [homepage] For more than three decades she has been a leading authority on the social implications of technology. She developed a privacy theory "contextual integrity," in books and articles that has been cited thousands of times by academic and industry researchers across the disciplinary spectrum, and has influenced lawmakers around the world, including in the US, Europe, India, and China.

Patrick Parham is a Ph.D. student at the College of Information Studies, University of Maryland (UMD). He has been studying advertising and media technology, and proposals addressing the deprecation of third-party cookies. Patrick previously worked in the programmatic advertising industry.

PART I: Privacy Beyond Consent

Re Q.73 The Commission invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices. Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? How should the Commission evaluate its effectiveness? Also, Q.90 on plain language explanations, Q.12 on harms to different parties.

The FTC ANPR document provides an impressively complete review of evidence demonstrating that terms of service and "notice and consent" approaches, have utterly failed as the touchstone for determining unfair or deceptive data practices. To these arguments we add the following considerations:

- Meaningful consent is impossible and cannot serve as the sole gatekeeper because data flow policies are beyond individual cognitive capacity (as documented in the ANPR). Furthermore, an empirical research study of privacy policies demonstrated that "words-on-a-page" can deceptively oversimplify the amount of content consumers are required to absorb. In one illustration, the authors demonstrate that two sentences in Facebook's privacy policy encapsulate 128 distinctive data flows (Shvartzshnaider et al., 2019).

- *Responding to Q.90 about requiring plain-spoken explanations:* For this reason, "plain-spoken explanations" offer no remedy. Nissenbaum's "transparency paradox" asserts that no privacy policy, which is simple enough for the layperson to follow, captures the full extent and significance of data practices; and any policy comprehensive enough to capture the full extent and implications of data practices would be incomprehensible to the layperson (Nissenbaum, 2011). Accordingly, trendy privacy "nutrition labels," eviscerated by the first horn of the dilemma, offer no basis for meaningful consent and are not a solution to fundamental commercial surveillance problems.

- When individuals do grant consent, it is likely granted to what they *expect* data practices to be, and not what the data practices, in fact, are. Kirsten Martin's brilliant article demonstrates that when people read a typical privacy policy, they take away from it that a company's data practices conform with (reasonable) expectations and NOT with what literally is stated in the policy, in the event the two differ (Martin, 2015).

- As a result, the use of the term "privacy policy" itself can be a deceptive practice, if it omits baseline protections that consumers expect (Turow, 2018; Turow et al., 2007, 2018).

- Consent may not only be hard, it may also be irrelevant. Barocas & Nissenbaum (2014) demonstrate that:

- It may be impossible, at the time of consent, to state what may be inferred, given continuous accrual of data and novel methods.
- More problematically, even if a person withholds consent, the information in question may be inferred if others with similar profiles do grant consent. This number of consenters can be very small. This is an end run around consent.

Moreover, technically driven replacements for invasive data practices may turn out to be even more invasive than their predecessors if they are not grounded on sound conceptions of privacy. Sivan-Sevilla & Parnham (2022), for instance, show how supply side platforms' (SSP) cookie replacements for identifying consumers by the online advertising industry may potentially result in far worse privacy outcomes for consumers, by allowing advertising platforms greater ability to surveil and "single out" individuals (Sivan-Sevilla & Parham, 2022).

PART II: Contextual Integrity: Privacy as a Positive Value

Our comprehensive approach for regulating consumer surveillance pivots around a positive definition of privacy as *the appropriate flow of information,* placing front and center what it is that privacy promotes, instead of what it prevents. According to the theory of contextual integrity (CI), an information flow is appropriate if it conforms with informational norms of respective social domains. If norms are consistently disrupted by novel data practices frequently due to new sociotechnical systems, or have not yet formed, appropriateness is established through systematic evaluations of legitimacy (Nissenbaum, 2004, 2009, 2015, 2018). CI has featured in policy discussions for some years, most notably in the *2012 Consumer Privacy Bill of Rights* issued by the Obama White House Department of Commerce.[4]

Contexts: Social domains (or "contexts"), are characterized by sets of roles, information types and guiding norms, including those governing information flows. However, the **most fundamental**

[4] Obama White House Department of Commerce, Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the Global Digital Economy, https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

defining feature of social contexts are the ends, purpose, and values around which contexts are oriented. Contexts, as defined in CI, play a similar role in our thinking about privacy regulation as the notion of sectors has played.[5]

Informational norms: CI informational norms are characterized by five parameters: data subject, sender, and recipient (collectively referred to as the actors), information type (or attribute), and transmission principles (the conditions that constrain data flow from senders to recipients). For example, when a judge compels a witness to answer a question, the recipients are those present in court (or with access to records), the sender is the witness, the subject is whomever the information is about, the information type is whatever the witness says, and, "compulsion" is the transmission principle. To describe information flows for purposes of establishing whether privacy has been respected, it is critical to specify values for all five parameters. Failing to do so results in ambiguity, unless missing values are clearly understood. Accordingly, when creating trade regulations allowing or prohibiting certain practices, rules must specify values for the five CI parameters.

Legitimacy of privacy rules: CI recognizes two main sources of legitimacy for privacy rules (and data practices.) First, rules (and data practices) may gain legitimacy from their conformance with entrenched societal norms. Empirical methods offer effective means for uncovering such norms. Second, rules, data practices, and norms themselves may earn legitimacy (or lose legitimacy) through an evaluation process that considers (i) all relevant interests, including stakeholders and other affected parties (e.g. balancing, trading off, etc.); (ii) societal values (e.g. fundamental liberties, justice, etc.); and (iii) contextual functions, ends, purposes, and values. **Privacy as contextual integrity secures and promotes positive societal and contextual values.**

Below, we draw on CI to address ANPR questions.

[5] See: H. Nissenbaum (2015) "'Respect for Context': Fulfilling the Promise of the White House Report," In *Privacy in the Modern Age: The Search for Solutions,* Eds. M. Rotenberg, J. Horwitz, J. Scott, New York: EPIC/The New Press, 152-164. Available here.

Re Q.13 - 23 on commercial surveillance practices for children and Q.79 on different consent standards for different vulnerable populations.

Society must always consider the vulnerabilities of particular sub-populations, such as children and teens, individuals with disabilities, low-wage workers, etc. Contextual thinking integrates these and other vulnerabilities that attach to the different capacities of all individuals in relation to data processors. Children, to be sure, are vulnerable in certain ways, but patients, in healthcare domains, are vulnerable in other ways, as are workers in an employment context, students in educational contexts, and so on. Vulnerabilities are often not absolute but emerge from many types of unbalanced circumstances. Diverse considerations are based not only on the respective roles of data subjects; they depend, as much, on the capacities and roles of the data recipients. Therefore, children deserve a special FTC oversight, as discussed in FTC's Q.15 *regarding protections for children for services not targeted towards children*. They should be perceived as data subjects that are at the bottom end of asymmetries of power, knowledge, and resilience when it comes to consumer surveillance harms.

Re Q.38 on commercial surveillance practices such as fingerprinting, facial recognition, etc. and Q.10 on kinds of data to be subject to new regulation rules.

For similar reasons, CI does not flag specific types of data for special protection without specifying other, relevant contextual factors. It disagrees with other approaches that circumscribe particular categories of information for highly restrictive treatment and other categories for laxer treatment, without consideration of contextual factors, such as, sender, recipient, etc. Empirical evidence, demonstrating that survey respondents are highly discriminating in evaluating data practices based on all five factors (parameters), supports the CI perspective (Martin & Nissenbaum, 2017a, 2017b, 2019).

Biometric data (e.g. DNA, facial recognition, etc.) is likely to accrue numerous constraints because of its inferential and historical links with many other types of data. Nevertheless, from the point of view of CI, it is not uniquely in a class by itself. Rules governing biometric data need to specify values for the other parameters, and evaluated in terms of how effective they are in promoting balanced stakeholder interests and social and contextual ends and values. Data flow rules lacking

a complete parameterization may harbor confounding variables. Due to ambiguity in their interpretation, they may either over- or under-constrain data flows (Martin & Nissenbaum, 2017a).

***Re Q.24 on costs and benefits*.**

It follows from CI that assessments of costs and benefits should not be limited only to those of individual stakeholders, particularly data subjects, or even other individuals implicated by data flows from data subjects, e.g. family members or those with matching profiles (Barocas & Nissenbaum, 2014). Instead, costs and benefits to societal and contextual ends should be included in assessments. Public health should be included in the assessment of health data flows to public data authorities, sometimes even overriding individual benefits.

Re Q.12 ***To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?***

A contextual approach has much in common with a sectoral approach. To the extent that sectoral approaches yield substantive rules prescribing and proscribing specific flows of data, CI strongly favors sector-style approaches to rule-making, particularly those that take sectoral goals and values into consideration (and not merely a balancing of stakeholder interests). Sectoral approaches allow regulatory authorities to call to service a diversity of experts, not only technical experts, but experts in the specific sectors – teachers, superintendents, learning psychologists, etc. – to weigh in on sound data flow rules. In the ideal case, sectoral rules do not simply hand over decisions to individuals often least able to assess best practices. Importantly, US sectoral rules do suffer from this weakness.

It is of great interest that the FTC's ANPR calls out for special consideration of not only health and finance, but also data/information search, because in our view, digital information search services are akin to education and intellectual pursuit already recognized in the Bill of Rights as well as legislative acts, such as FERPA.

Comprehensive approaches are not able to give consideration to critical sectoral/contextual factors though they may have a role to play in high level declarations that assign basic rights to appropriate flows.

Re Q.77 and Q.78 on notice and choice, and Q.84 on transparency and disclosure requirements.

If substantive rules, per our recommendation, are shaped by area (sectoral, contextual) experts and stakeholder representatives are developed and enforced by regulators, there is a lesser, and more reasonable burden on consumers, who are typically, **un**informed and manipulable (as demonstrated in the literature). In turn, disclosure to individual data subjects play a less critical role and may be keyed to individual preferences rather than legitimate interests.

We acknowledge that formulating substantive restrictions that serve legitimate contextual ends and values, is more difficult than a one-size-fits-all approach (like the notice and choice paradigm that simply punts the decision to actors who are least informed). The payoff, however, is a more robust, more fair, more balanced approach than consent-based approaches, in which individuals are fully burdened with little insight into actual practices, or their consequences.

Re Q.43 on limiting collection, use, and retention of data, esp. compatible with specific services; Q.45 on purpose limitations and Q.46 on data minimization and purpose limitation by service or sector.

We revert to terminology found in traditional renditions of the fair information practice principles (FIPPs), which cites, “purpose specifications” and “use limitations.” A “data processor” (collector, user, holder, or distributor, etc.) must (1) **specify** the purposes of their activity; and (2) data uses are **limited** by these purposes. Initially, privacy was thought to be adequately respected as long as purpose was specified and uses were limited accordingly. Fast forward to the present time, this interpretation is woefully inadequate because it allows a wide-open door for industry incumbents to specify purposes that would allow almost any use.

Contextual Integrity (CI), by contrast, prescribes that the purposes of data processing and data uses be constrained by substantive, legitimate informational norms. As noted above, appropriate flow depends on the context in which a service is operating, the types of information, and the capacities in which data subjects and data processors are acting. We would expect that legitimate purposes and uses would differ as contexts and respective factors differ. Substantive constraints may be prescribed, in general terms, through sectoral (or contextual) law and/or regulation, and may be further elaborate in more nimble forms of rule-making focusing, e.g. on educational apps, or search services, wellness apps and IoT devices, etc.

By analogy, food safety certifications is a required baseline before food can be offered to consumers. Special qualifications are required for surgeons to perform surgery. These substantive restrictions, may be supplemented by opt-in user choice, e.g. selecting a mayonnaise brand, or a particular surgeon.

Crucially, use limitations are those that conform with specified purposes *only if* the purposes specified are legitimate ones, that is, aligned with legitimate contextual norms.

Data minimization, a concept derived from privacy engineering and privacy-by-design can work as a principle of rule-making only if this is qualified by purpose limitations based on legitimate purposes, as already noted above. For example, we have sound ideas on how to minimize data for search (intellectual inquiry and education), finance, and health, but these are not the only areas where data minimization must be subjected to the requirements of legitimate contextual data flow norms. **By itself,** a principle of data minimization is arbitrary, and unjustifiable, as a guide to rule-making for privacy (though it may help contain security risks due to breaches, for example.)

In short, contextual integrity supports data minimization tailored to *balanced* outcomes for stakeholders and for societal and contextual public good.

An approach to rulemaking based on the principles of Contextual Integrity proceeds by:

1. Identifying a context's purposes, values, and functions. (Why does a context, sector, or industry exist, and what societal purpose does it achieve?)

2. Enumerating data flows generated by common data practices by describing these flows in terms of the five contextual parameters.
3. Evaluating these data flows against people's expectations of appropriate practice.
4. Establish the legitimacy of practices and data flows by evaluating them in terms of their capacities to promote societal and contextual purposes and values.
5. Develop regulatory strategies to encourage data practices that promote contextual ends and purposes either via enforcement of rules, or other incentives.
6. Develop regulatory strategies to enable continuous audits of data practices, particularly those generated by new technical systems.

Identifying a context's purposes, values, and functions: Data is not just data. Depending on context, data is educational data, financial data, health care data, etc. Educational data flows should enable effective learning. Investment data flows facilitate the efficient allocation of capital to form frictionless partnerships between investors and investees. Health care data flows exist to improve health outcomes. Each of these contexts has distinct guiding values and purposes. For example, the purposes of healthcare include the diagnosis and treatment of illnesses, medical research, and public health. Rather than focusing on consent, type of data, or individual purposes, shifting to "information flows" as the unit of analysis enables a deeper and more accurate understanding of the purposes and values enabled through data. This allows for a proper evaluation of practices based on the societal norms that need to be respected in the given context.

Enumerating data flows of common practices: As mentioned, above, a data flow is defined by five parameters: sender, recipient, data subject, information type, and transmission principle. This parameterization is a prerequisite for evaluating whether or not that data flow preserves societal norms in its given context, and therefore, respects privacy. Returning to our health care example, one potential flow is a patient getting a prescription for medication filled. A patient's (subject) physician (sender) can send a pharmacist (recipient) a prescription (attributes, potentially including insurance information) electronically for the purpose of prescription provision (transmission principle). Note that this flow is distinct from a doctor writing the patient a physical prescription that the patient then takes to the pharmacy. Both of these flows are appropriate and consistent with the norm that, in the healthcare context, the safe sharing of sensitive information that improves health outcomes should be encouraged. Note that this norm, in addition to including many of the

injunctions against data flow typically associated with privacy requirements, also actively supports innovation and reducing friction for consumers. That is, the norm promotes prohibitions (e.g., prescription information cannot be used for marketing purposes) and innovation (e.g., streamlining the processing of valid prescriptions with well-regulated apps and identity standards).

Establish the legitimacy of practices and data flows by evaluating them in terms of their capacities to promote societal and contextual purposes and values: Data flows should be evaluated according to how they achieve societal purposes and values. In the earlier prescription example, certain controls are implemented to ensure societal purposes are achieved while reducing the risk of societal harm. Those controls include licensing for both the physician and pharmacist, the prescription must contain certain information, and electronic communications must be secure. If all the conditions are met, the flow is valid. Most flows under consideration for rulemaking will not be as straightforward. Consider the case of disease diagnosis information. Doctor-patient confidentiality means that in most cases this information cannot be shared with government agencies, but in the case of an epidemic, the public health interest may prevail. Larger societal values, like ensuring that such information flow does not unduly increase the risk that certain groups are not discriminated against, must also be weighed.

Develop regulatory strategies to encourage data practices that promote contextual ends and purposes either via enforcement of rules, or other incentives: Some of the practicalities of putting our notion of privacy and its value into practice are detailed in Section III below. We focus on the enforcement process, and argue that ensuring that data practices are promoting contextual ends and purposes can be encouraged by empowering additional stakeholders in the enforcement process. We specifically call for importing (1) mandatory complaints and the (2) institutionalization of civil rights organizations in the enforcement process from the European Data Protection regime. We also call for the FTC to produce machine-readable enforcement data, enabling academics and civil society to trace enforcement trends over time and highlight alarming patterns.

Develop regulatory strategies to enable continuous audits of data practices, particularly those generated by new technologies: The regulatory challenge of “keeping pace” with technological change is outlined and addressed in Section IV below. We suggest ways for “designing and building adaptability” into rulemaking processes for commercial surveillance and introduce a model

that triggers the regulatory process across three “learning cycles,” providing ways to overcome some of the current challenges with regulating surveillance-based industries.

PART III: Policy Implementation: Standardizing Enforcement Data & Institutionalizing “Fire-Alarms” from Civil Rights Agencies

Relevant Questions:

To what extent should the Commission rely on third-party intermediaries (e.g., government officials, journalists, academics, or auditors) to help facilitate new disclosure rules? **[Q. 87]**

Which, if any, mechanisms should the Commission use to require or incentivize companies to be forthcoming? Which, if any, mechanisms should the Commission use to verify the sufficiency, accuracy, or authenticity of the information that companies provide? **[Q. 85]**

How can the Commission's expertise and authorities complement those of other civil rights agencies? How might a new rule ensure space for interagency collaboration? **[Q. 72]**

The challenge for new consumer surveillance rules is not only in the proper design of policies according to the Contextual Integrity framework. It is also in bringing these new policies into life and creating a culture of compliance among market surveillance actors. To do so, we propose three steps:

- Create machine-ready enforcement data and invite academics and civil society to develop tools for measuring and tracing FTC enforcement trends over time [Q. 87].

- Shift from voluntary to mandatory-based complaints mechanism, through which the FTC is obligated to act upon consumers’ complaints. The agency would then pressure and potentially sanction companies to a greater degree, encouraging market actors to be forthcoming about their applied information practices [Q. 85].

- Institutionalize the involvement of civil rights agencies in the enforcement process by enabling the representation of data subjects by civil rights agencies in front of the FTC upon market surveillance harms [Q. 72]. Such a mechanism would create a space for collaboration between civil society groups and the agency, harnessing NGOs' privacy expertise and organizational capacities in advancing bottom-up policy enforcement and pressuring companies to comply.

Implementation of consumer surveillance rules takes a village. First, with many market actors shifting towards surveillance-oriented business models in our data-capitalist economy (Sadowski, 2020; Sivan-Sevilla, 2021), a broad array of actors are becoming subject to consumer surveillance rules, challenging FTC's capacities to actively enforce the law across the market. Just like Data Protection Authorities in the EU, the agency has to be selective in the cases it chooses to investigate, but at the same time, deter other actors and create a "culture of compliance" at length from policy targets (Sivan-Sevilla, 2022). Therefore, the discretion of FTC enforcement agents is crucial for an effective consumer surveillance regime and should be constantly monitored and evaluated through civic technologies developed by third parties (Q.87). We therefore call for a standardized and "machine-ready" enforcement data to be published and monitored by academics and civil society over time (See an emerging attempt to do so for the GDPR: Supreeth, 2022).

Second, the ability to raise "real-time" fire alarms on violations of consumer surveillance rules becomes central to the enforcement process. The rapid institutionalization of commercial surveillance led to private-interest implementation of policy values by corporations that mediate digital services for end users. Companies that enable social media networks, digital advertising, mobile app stores, monetization of websites, and etc., at the heart of our digital economy, are rarely scrutinized by public authorities, who lack capacities and expertise in complex technological settings (See an example from the advertising industry: Sivan-Sevilla & Parham, 2022). There is a time lag between the emergence of a new consumer surveillance practice and the existing, sticky, public institutional arrangements reacting to it. Such time lag provides market actors a gray space to experiment with new business models and data governance decisions, creating 'lock-in' effects for newly introduced surveillance practices, and turning them into acceptable norms that our society is struggling to diverge from.

To bridge this burning implementation gap we propose to enable a mandatory “complaints-based” mechanism, through which consumers can file complaints to the FTC on market surveillance harms. The FTC will be obligated to further investigate consumer cases and address the broad and dynamic array of harms. This might pressure other actors to be more transparent about their data practices (Q.85), creating greater FTC deterrence across the market. Currently, US consumers can file complaints to the Commission at FTC.gov, but there is no obligation for the Commission to investigate and follow-up on individual complaints.

Furthermore, we are proposing the institutionalization of civil rights agencies in the policy enforcement process (Q.72). Similar to Article 80 of the European GDPR, which foresees that data subjects can be represented by a non-profit association, we propose to enable the representation of data subjects by civil rights agencies in front of the FTC upon market surveillance harms. Those NGOs could officially file complaints with the FTC, nudging the agency to pay attention to market surveillance harms they are potentially not yet familiar with. Such privacy-minded civil society groups, like the Electronic Frontier Foundation (EFF) or the Electronic Privacy Information Center (EPIC) in the US, are far better equipped than individual consumers to strategically focus on issues and potential violations of market surveillance rules with broad social impact. Based on examples emerging from Europe, civil society actors are essential in bringing strategic market surveillance gaps in front of regulatory agencies. NGOs were found to inject technical expertise, legal knowledge, and organizational capacities to the privacy enforcement process, contributing to the efforts of regulators in creating a culture of compliance across market actors (Borohovich et al., 2022; Jang & Newman, 2022). In addition to reacting to more obvious harms, privacy focused NGOs can perform dedicated research and proactively identify issues and harms that individuals or more traditional consumer rights organizations might miss, including in sectors where discrimination might be prevalent but not widely known.

Just as privacy NGOs in Europe have increasingly worked transnationally (Borohovich et al., 2022), bringing NGOs into the fold in the US could enable cases that address issues spanning the patchwork of state, federal, and international data privacy laws and regulations. Importantly, such a network of privacy focused, cooperative, proactive NGOs in Europe did exist before GDPR’s Article 80, but their impact on the enforcement process was rather indirect as they were fighting for attention from regulators and tech companies. Through the formal institutionalization of civil rights

agencies in the enforcement process, the FTC would gain tremendous assistance in addressing prevailing market surveillance harms.

PART IV: Adaptive Regulatory Processes for Market Surveillance Dynamics

Relevant Question: ***How should the Commission account for changes in business models in advertising as well as other commercial surveillance practices? [Q.95]***

Beyond the design of new contextual privacy rules, the standardization of enforcement data, and the institutionalization of civic actors in the enforcement process, regulating consumer surveillance requires divergence from the traditionally static and slow regulatory processes that often fail to respond to dynamic market conditions in technological contexts (Marchant et al., 2013). According to the public policy literature, policy changes are usually crisis-driven, inspired by events that captured the limited attention of policymakers across policy arenas (Baumgartner et al., 2018; Lindblom, 1959). Such sticky policy processes are in sharp contrast to the rapidly evolving societal and technological environments.

In such a dynamic policy arena, any rulemaking that does not adequately account for the context(s) of data practices in an adaptive way runs the risk of obsolescence. For example, with tech companies moving into the spaces of finance, healthcare, search, and social media, we need to adapt regulation to these new actors. While it may not be the case that a commercial health app is treated exactly as a traditional healthcare provider, since the service of the commercial app are similar to those of traditional actors, we need to think about sui generis rules that serve individual users of these apps as well as the robustness of healthcare broadly conceived, exactly as was considered when developing HIPAA and HITECH.

Scholars of regulation have long called for models of “adaptive regulation” to regulate upon uncertainty and complexity (Bennear & Wiener, 2019; Brass & Sowell, 2021; McCray et al., 2010; Swanson et al., 2010). Regulation should not be considered as a single attempt to change undesired market consequences, but as a continuous process that learns, adapts, and changes upon market dynamics. Instead of “regulate-and-forget” we call for an “adapt-and-learn” approach

to consumer surveillance. US companies have been taking advantage of stiff regulatory processes to escape oversight and conveniently locate themselves outside the scope of privacy rules and regulations. In healthcare for instance, health and wellness apps escape strict oversight, in what has been framed by Nissenbaum, Strandburg, and Viljoen (forthcoming) as "the great regulatory dodge" (See an example here: Privacy International, 2019). Moreover, market surveillance is becoming more sophisticated over time, using techniques that cannot be fully captured in a "one-time" policy design attempt (See for example Hill, 2020 on Clearview AI that was accidently regulated only in Illinois; Iqbal et al., 2020 on advanced digital fingerprinting of consumers; or Szymielewicz, 2019 on the increasingly sophisticated construction of consumer identities).

In order for the FTC to keep up with the dynamic commercial surveillance landscape (Q.95), we propose the application of adaptive regulatory approaches through three "regulatory learning cycles:"[6]

- Identification & analysis of new consumer surveillance risks.
- Real-time monitoring of known surveillance risk indicators to flag non-compliance.
- Constant validity assessments of current regulations.

The three learning cycles are described in detail in the following paragraphs. Each learning cycle can update the FTC regulations upon new information on an ongoing basis.

Creating new regulations upon new risks: The *first* adaptive cycle is the forward-looking identification and analysis of new surveillance risks. The FTC could institutionalize mechanisms for constant input from academics, privacy risk professionals, civil society organizations, and community leaders who are capable of highlighting surveillance risks the FTC is yet to be familiar with. The information-gathering process can potentially flag new market practices that are currently unregulated and highlight new avenues for consumer surveillance (See for instance Trimananda et al., 2021 about the privacy implications of VR technologies). The FTC will be committed to act upon the new knowledge, potentially update its rules, or at least publicly distribute alarms for consumers to be aware of potential new harms.

[6] Those cycles were originally developed for the climate crisis case by Dr. Lior Zalmanson and Dr. Ido Sivan-Sevilla and were adapted here for the consumer surveillance domain.

Updating existing thresholds upon new market behavior: The *second* adaptive cycle addresses FTC's learning through real-time monitoring of known surveillance thresholds. Such monitoring can include the independent tracing of data collected by third parties in popular mobile apps, or the comparison of changes in privacy policies of main digital service providers over time. It can also include the tracing of new identifiers used by the advertising industry and the sharing of those identifiers between websites. These are all just examples of potential surveillance indicators that the FTC and its networks can monitor regularly to assess compliance and act upon non-compliance.

Updating existing rules upon non-compliance: The *third* adaptive cycle is evolved around continuous validity assessments of FTC regulations that would help flag whether existing regulations are outdated. In contrast to the previous two learning cycles that monitor new and existing surveillance risks initiated by regulated companies, this cycle assesses the relevancy of FTC rules over time. Questions such as to what extent market actors can comply, or what is the level and likelihood of non-compliance, would help the FTC fine-tune existing rules to known market surveillance risks. In cases in which regulatory requirements are difficult to follow in practice, regulatory re-design may be triggered.

References

Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 44–75). Cambridge University Press. https://doi.org/10.1017/CBO9781107590205.004

Baumgartner, F. R., Jones, B. D., & Mortensen, P. B. (2018). Punctuated Equilibrium Theory: Explaining Stability and Change in Public Policymaking. In *Theories of the Policy Process* (4th ed.). Routledge.

Bennear, L. S., & Wiener, J. B. (2019). *Adaptive Regulation: Instrument Choice for Policy Learning over Time*. 37.

Berjon, R. (2021). *Pushing Back Against Privacy Infringement On The Web*. Smashing Magazine. https://www.smashingmagazine.com/2021/08/against-privacy-infringement-web/

Biddle, S., August 25 2021, M. S., & P.m, 12:33. (2021). *Little-Known Federal Software Can Trigger Revocation of Citizenship*. The Intercept. https://theintercept.com/2021/08/25/atlas-citizenship-denaturalization-homeland-security/

Borohovich, I. M., Newman, A., & Sivan-Sevilla, I. (2022). *The civic transformation of data privacy implementation in Europe*. OSF Preprints. https://doi.org/10.31219/osf.io/vrw5y

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*, *15*(4), 1092–1110. https://doi.org/10.1111/rego.12343

Choi, H., Mela, C. F., Balseiro, S. R., & Levy, A. (2020). Online Display Advertising Markets: A Literature Review and Future Directions | Information Systems Research. *Information Systems Research*, *2*(31), 556–575. https://doi.org/10.1287/isre.2019.0902

Hill, K. (2020). The Secretive Company That Might End Privacy as We Know It—The New York Times. *New York Times*. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Iqbal, U., Englehardt, S., & Shafiq, Z. (2020). *Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors* (arXiv:2008.04480). arXiv. https://doi.org/10.48550/arXiv.2008.04480

Jang, W., & Newman, A. L. (2022). Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation*. *JCMS: Journal of Common Market Studies*, *60*(2), 283–300. https://doi.org/10.1111/jcms.13215

Lindblom, C. E. (1959). The Science of “Muddling Through.” *Public Administration Review*, *19*(2), 79–88. https://doi.org/10.2307/973677

Marchant, G. E., Allenby, B. R., & Herkert, J. R. (2013). *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*. Ingramcontent.

Martin, K. (2015). Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online. *Journal of Public Policy & Marketing*, *34*(2), 210–227. https://doi.org/10.1509/jppm.14.139

Martin, K., & Nissenbaum, H. (2017a). Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables. *Science and Technology Law Review*, *18*(1), Article 1. https://doi.org/10.7916/stlr.v18i1.4015

Martin, K., & Nissenbaum, H. (2017b). *Privacy Interests In Public Records: An Empirical Investigation* (SSRN Scholarly Paper No. 2875720). https://doi.org/10.2139/ssrn.2875720

Martin, K., & Nissenbaum, H. (2019). *What Is It About Location?* (SSRN Scholarly Paper No. 3360409). https://doi.org/10.2139/ssrn.3360409

McCray, L. E., Oye, K. A., & Petersen, A. C. (2010). Planned adaptation in risk regulation: An initial survey of US environmental, health, and safety regulation. *Technological Forecasting and Social Change*, *77*(6), 951–959. https://doi.org/10.1016/j.techfore.2009.12.001

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 119.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Nissenbaum, H. (2015). Respect for context as a benchmark for privacy online: What it is and isn't. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 278–302). Cambridge University Press. https://doi.org/10.1017/CBO9781107280557.016

Nissenbaum, H. (2018). Respecting Context to Protect Privacy: Why Meaning Matters. *Science and Engineering Ethics*, *24*(3), 831–852. https://doi.org/10.1007/s11948-015-9674-9

Privacy International. (2019). *Your mental health for sale | Privacy International*. https://privacyinternational.org/campaigns/your-mental-health-sale

Privacy International. (2022). *Shining a light on the hostile environment*. Privacy International. http://www.privacyinternational.org/news-analysis/4907/shining-light-hostile-environment

Sadowski, J. (2020). *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Ove r the World*. The MIT Press.

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2019). Going against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis. *Proceedings of the*

AAAI Conference on Human Computation and Crowdsourcing, *7*, 162–170. https://doi.org/10.1609/hcomp.v7i1.5266

Sivan-Sevilla, I. (2021, August 12). *Can We Diverge From the Path of Digital Surveillance?* SMERCONISH. https://www.smerconish.com/exclusive-content/can-we-diverge-from-the-path-of-digital-surveillance

Sivan-Sevilla, I. (2022). Varieties of enforcement strategies post-GDPR: A fuzzy-set qualitative comparative analysis (fsQCA) across data protection authorities. *Journal of European Public Policy*, *0*(0), 1–34. https://doi.org/10.1080/13501763.2022.2147578

Sivan-Sevilla, I., & Parham, P. T. (2022). *Toward (Greater) Consumer Surveillance in a 'Cookie-less' World: A Comparative Analysis of Current and Future Web Tracking Mechanisms*. SocArXiv. https://doi.org/10.31235/osf.io/rauwj

Supreeth, S. (2022). *GDPRxiv*. GDPRxiv. https://www.gdprxiv.org

Swanson, D., Barg, S., Tyler, S., Venema, H., Tomar, S., Bhadwal, S., Nair, S., Roy, D., & Drexhage, J. (2010). Seven tools for creating adaptive policies. *Technological Forecasting and Social Change*, *77*(6), 924–939. https://doi.org/10.1016/j.techfore.2010.04.005

Szymielewicz, K. (2019, January 25). *Your digital identity has three layers, and you can only protect one of them*. Quartz. https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/

Trimananda, R., Le, H., Cui, H., Ho, J. T., Shuba, A., & Markopoulou, A. (2021). *OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR* (arXiv:2106.05407). arXiv. https://doi.org/10.48550/arXiv.2106.05407

Turow, J. (2018, August 20). Opinion | Let's Retire the Phrase 'Privacy Policy.' *The New York Times*. https://www.nytimes.com/2018/08/20/opinion/20Turow.html

Turow, J., Hennessy, M., & Draper, N. (2018). Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003–2015. *Journal of Broadcasting & Electronic Media*, *62*(3), 461–478. https://doi.org/10.1080/08838151.2018.1451867

Turow, J., Hoofnagle, C. J., Mulligan, D. K., Good, N., & Grossklags, J. (2007). *The Federal Trade Commission and Consumer Privacy in the Coming Decade* (SSRN Scholarly Paper No. 2365578). https://papers.ssrn.com/abstract=2365578

Zhang, N., Wang, C., Karahanna, E., & Xu, Y. (2022). Peer Privacy Concerns: Conceptualization and Measurement. *MIS Quarterly*, *46*(1), 491–530. https://doi.org/10.25300/MISQ/2022/14861

✉ **Ido Sivan-Sevilla**
University of Maryland
College Park, MD
sevilla@umd.edu
More Info >

✉ **Helen Nissenbaum**
Cornell Tech
New York, NY
hn288@cornell.edu
More Info >

✉ **Patrick Parham**
University of Maryland
College Park, MD
pparham@umd.edu
More Info >