IDO SIVAN-SEVILLA

To Save Society from Digital Tech, Enable Scrutiny of How Policies Are Implemented

In May 2023, the leaders of the G7 nations called for "guardrails" to limit potential damage caused by artificial intelligence (AI). Days later, the CEO of OpenAI, the company that developed ChatGPT, advised Congress to pass safety regulations over AI models. In 2022 alone, nine AI-related US federal laws and 21 state-level laws were passed. Since 2015, AI has been discussed with growing frequency in congressional committees: the term was mentioned 73 times in committee reports produced in 2021–2022 by the House and Senate. Meanwhile, the European Union is working out the Artificial Intelligence Act to minimize what threats the application of machine learning might pose to privacy, security, and democratic values.

The frenzy of policymaking is not only over AI. The European Union invested almost seven years of intense work in crafting the General Data Protection Regulation (GDPR) text, aiming to protect EU citizens' privacy. The European Union has also been working recently to pass the Digital Services and Digital Markets Acts and increase liability and competition in online markets. Several US states are about to enforce new GDPR-like rules, and a new federal privacy law is potentially on the horizon. On the cybersecurity front, 36 US states enacted new legislation in 2021 alone to demand more protection and transparency.

Articles in *Nature*, *Wired*, *The Economist*, at the Brookings Institution, and elsewhere have called for the creation of new crosscutting agencies to figure out how to handle new technologies and design policies that can prevent social harm from the latest developments, but each proposal overlooks a crucial ingredient for success: the bits and bytes of how technology policy is *implemented*. I study the bridge between computer science and public policy, trying to understand how fast-moving information technology is governed. Time and again, good-faith policies are thwarted by those who put policy into practice.

A spotlight on implementation

There are many examples of well-intentioned tech policies failing to protect society. Investigative journalists and activists have uncovered how hospitals sent sensitive medical information to Facebook, potentially violating the Health Insurance Portability and Accountability Act, which regulates the use of patient health data. They have also revealed how machine learning software deployed by police departments has led to wrongful arrests, violating citizens' rights under the Fourth Amendment, which bans unreasonable searches and seizures. Researchers found that advertising companies are using sophisticated practices such as "cookie respawning" with "browser fingerprinting" to dodge legal requirements and so maintain surveillance on users over time. The list goes on. Despite plenty of privacy and cybersecurity laws enacted around the world, data breaches and privacy abuses are frequent and harmful.

Innovation scholars Gary Marchant and Wendell Wallach have called for the creation of government coordination committees to design policies for fast-moving technologies; however, there is little discussion about how to create accountability when implementing tech policies. Decades of research exploring policy implementation across diverse areas consistently shows how successful implementation allows policies to be adapted and involves crucial bargaining. But this is rarely understood in the tech sector. For tech policies to work, those responsible for enforcement and compliance should be overseen and held to account. Otherwise, as history shows, tech policies will struggle to fulfill the intentions of their policymakers.

Scrutiny is required for three types of actors. First are regulators, who convert promising tech laws into enforcement practices but are often ill-equipped for their mission. My recent research found that across Europe, the rigor and methods of national privacy regulators tasked with enforcing

the European Union's GDPR vary greatly. The French data protection authority, for instance, proactively monitors for privacy violations and strictly sanctions companies that overstep; in contrast, Bulgarian authorities monitor passively and are hesitant to act. Reflecting on the first five years of the GDPR, Max Schrems, the chair of privacy watchdog NOYB, found authorities and courts reluctant to enforce the law, and companies free to take advantage: "It often feels like there is more energy spent in undermining the GDPR than in complying with it." Variations in resources and technical expertise among regulators create regulatory arbitrage that the regulated eagerly exploit.

Tech companies are the second type of actor requiring scrutiny. Service providers such as Alphabet, Meta, and Twitter, along with lesser-known technology companies and their clients, mediate digital services for billions around the world but enjoy considerable latitude on how and whether they comply with tech policies. Civil society groups, for instance, uncovered how Meta was trying to bypass the GDPR and use personal information for advertising. Some of the most incriminating revelations about tech company practices are only known thanks to whistleblowers like former Facebook employee Frances Haugen, who testified that Meta knew about the risks Instagram poses to the mental health of teenage girls as well as the prevalence of human traffickers on its platforms. In another case, Google agreed to pay nearly $400 million for breaking consumer protection laws since at least 2014 by surreptitiously recording people's movements and locations in the United States and selling that data to advertisers. A 2023 antitrust lawsuit filed by the US Department of Justice alleges that Google monopolized digital advertising technologies, dictating its business preferences over who can buy and sell ads online and forcing publishers and advertisers to adopt the company's tools.

State agencies, the third class of actor requiring scrutiny, include police departments, surveillance agencies, and those administering public benefits. These agencies regularly apply technological tools outside public view to monitor citizens and to make decisions about arrests, incarceration, benefit eligibility, and more, all with significant consequences for individuals. After 9/11, the George W. Bush administration launched digital surveillance programs that were later revealed by the whistleblower Edward Snowden and ultimately found to be illegal. In another technology scandal, an investigative reporter from the *New York Times*, Kashmir Hill, found that law enforcement agencies have been using the facial recognition software Clearview AI, which collects highly sensitive biometric information on individuals from all over the world without their knowledge or consent. Such abuse of biometric information for law enforcement was found to be illegal in Canada, France, Greece, Austria, and the United Kingdom. Other harmful uses of technology by state agencies that have been uncovered by journalists include machine learning algorithms that apply racial bias when sentencing people convicted of crimes and exclude eligible populations from health care and unemployment benefits.

What unites these three disparate policy implementers is the gap between their responsibilities to prevent technological harms and the tools society can use to scrutinize their work. Every actor described above can be lax in how they regulate and use harmful technologies because there are no systems or policies in place to ensure digital accountability.

Achieving scrutiny

The key to scrutinizing how technology is deployed and regulated is civic technologies: software and data gathering tools created by community-led efforts to enhance the public good. These can provide technical and automated monitoring mechanisms that help politicians, judges, data subjects, intelligence and law enforcement oversight committees, and citizens hold technology to account. Civic technologies can provide the means to understand how a given technology operates and offer the required transparency to bring consequences for poor practices. Already, monitoring by activists and academics is having an effect, revealing how great the need is for coordinated, supported efforts to follow tech policy implementation.

Regulators. One tool to hold regulators to account involves crowdsourcing. For example, NOYB has built GDPRhub, a wiki that functions as a repository of GDPR-related decisions and knowledge, updated by the public, that monitors more than 100 relevant webpages across European states. Another initiative from researchers at the University of Iowa, called GDPRxiv, is an automated information archive system that collects and curates GDPR rulings, judgements, reports, and official guidance. Researchers can use these tools to reveal different privacy enforcement cultures across Europe, surface blind spots and enforcement deficits, and trace their improvement over time.

In my experience, regulators resist scrutiny rather than invite it; my work to collect data from national privacy regulators to understand GDPR enforcement took more than a year and required continuous nudging to get only a 58% response rate (18 out of 31 national privacy regulators in the European Union). An essential step is ongoing monitoring and evaluation of enforcement to understand how regulators operate. When the US Federal Trade Commission sought public input on harmful commercial surveillance and lax data security practices, my colleagues and I submitted suggestions calling for agencies to produce machine-readable enforcement data that can be collected and analyzed over time.

Tech companies. There already are some open and publicly available tools for inspecting tech companies' compliance with policies. For instance, the Open Web Privacy Measurement tool quantifies how online actors collect information on web users. As of late 2022, it had been used in 70 peer-reviewed

publications. I used it in my own project to understand how web trackers identify users across different social contexts, highlighting the importance of understanding web privacy in a contextual way. The tool also helped researchers reveal the techniques and volume of tracking by online advertisers, questioning whether the online advertising industry was complying with privacy policies. Another set of tools comes from those developing dedicated browser extensions or web services for consumers, helping to highlight how web trackers breach users' privacy.

For mobile apps, researchers have developed AppCensus, a tool that enables inspection of app code and operation, capturing the information collected and sent from mobile devices to tech companies. The tool was used to show how well Android app developers follow stipulations of the California Consumer Privacy Act.

To understand anticompetitive behavior in Google and Amazon search results, The Markup, a nonprofit investigative journalism organization, developed technology to analyze Google's seemingly objective search results, revealing how much space was devoted to Google's own services. The team also created tools to examine how Amazon prioritizes its own products in Amazon search results.

State agencies. Technological scrutiny over state agencies is tricky. Law enforcement personnel may use facial recognition or other intrusive tools before proper oversight is established. For example, Israeli police have been accused of using Pegasus spyware, a hacking tool developed by Israel's NSO Group, to search citizens' mobile phones for intelligence without active investigations or warrants. In addition, when asked for information under open records requests, agencies may claim that trade secrets and nondisclosure agreements exempt them from even declaring whether they have that information, let alone providing it.

Nonetheless, researchers can develop tools to learn what government entities are doing. One spectacular example is the University of Toronto's Citizen's Lab, which has exposed the ways that many countries have used Pegasus software to hack the phones of journalists, activists, and opposition parties. In a separate effort, I have developed a tool with colleagues to continuously monitor and visualize the vulnerability of publicly facing devices operated by local government systems in the United States. We found databases in health centers that were vulnerable to unauthorized access, raising questions of whether local government services can comply with cybersecurity requirements. These sorts of independent projects from researchers and journalists demonstrate the potential for using tools to track policy compliance across state agencies and hold agencies to account.

Although these innovations are encouraging, the most alarming technological practices are arguably conducted on the server side, away from the public eye. Powerful tech companies interested in maintaining their reputations are unlikely to reveal their practices, nor are powerful state actors who often promote "greater" security goals and threats at the expense of privacy concerns. Observations that are restricted to the client side offer a very limited view. New transparency obligations from all three types of actors—and consequently better tools to capture and analyze the decisions of tech policy implementers—are required.

Illuminate the black box

Today, tech policy implementation operates mainly in a "black box." Society has no access to the considerations regulators apply when choosing how to enforce the law, no access to the data collected and algorithms used when companies make decisions about people, and no access to the various ways the government applies technology for its own purposes. Opaque technology can never promote accountability.

Seeing inside this black box will require regulators, tech companies, and government agencies to be transparent about how they use and oversee technology. Enforcement agencies should adhere to public accountability standards and continuously provide information on their enforcement decisions and activities. Digital service providers should open their algorithms to the public eye, enabling others to scrutinize their implementation choices. Government agencies should create a repository of government technologies and their applications, just like federal agencies have been starting to do through ai.gov, the website of the National AI Initiative.

To make sure such scrutiny is systematically applied, efforts to employ civic technologies must be coordinated and well-funded, with more transparency from regulators, enforcement agencies, and tech companies. Oversight entities should no longer trust companies and governments when they apply technology but instead join forces with researchers and civil society to increase accountability. These civic technologies are the missing tool to create a larger public discourse around tech governance decisions, providing new ways for regulators, tech companies, and state agents to face consequences when they fail to protect societal values.

Thirty years ago, legal scholar Lawrence Lessig argued that "code is law," meaning that how technology is designed governs how well it can protect social goods. Since then, technology has taken an alarming turn in determining people's opportunities, and yet people's opportunities to know how technology is designed have become more limited. But in a world that is increasingly defined by code, no code should be above the scrutiny of the law.

Ido Sivan-Sevilla *is an assistant professor of information studies at University of Maryland, where he develops measurements and theories of how society is governed across a range of cybersecurity, privacy, and machine learning issues.*