

How the Netherlands Is Taming Big Tech

Dutch privacy negotiators have spurred major changes at Google, Microsoft and Zoom, using a landmark European data protection law as a lever.

By **Natasha Singer**

To research this story, Natasha Singer, a technology reporter, spent weeks studying Dutch privacy audits of Google, Microsoft and Zoom.

Jan. 18, 2023

In 2021, privacy consultants working for two Dutch universities issued a critical report card on Google’s education apps, a set of classroom tools like Google Docs that are used by more than 170 million students and educators worldwide.

The audit warned that Google’s tools for schools lacked a number of privacy protections — like narrow limits on how the company could use students’ and teachers’ personal data — that were required by European law. Although the company addressed some of the concerns, the report said, Google declined to comply with Dutch requests to reduce a number of “high risks” cited in the audit.

It took a threat from the Dutch Data Protection Authority, the nation’s privacy regulator, to help break the deadlock: Dutch schools would soon have to stop using Google’s education tools, the government agency said, if the products continued to pose those risks.

Two years later, Google has developed new privacy measures and transparency tools to address the Dutch concerns. The tech giant now plans to roll out those changes to its education customers later this year in the Netherlands and elsewhere around the world.

Dutch government and educational organizations have had remarkable success in compelling Big Tech companies to make major privacy changes. Their carrot-and-stick approach engages high-level Silicon Valley executives in months of highly technical discussions and then makes it worth their while by negotiating collective agreements allowing firms to sell their vetted tools to different government ministries and the nation’s schools. And the Dutch efforts to prod change could provide a playbook for other small nations wrangling with tech superpowers.

For some U.S. tech companies, the Dutch imprimatur has now become a status symbol, a kind of seal of approval they can show regulators elsewhere to demonstrate they have passed one of Europe’s most stringent data protection compliance processes.

How the Netherlands, a small country with a population of about 17.8 million people, came to sway American tech giants is a David and Goliath story involving a landmark law, called the General Data Protection Regulation, that was put into effect in 2018 by European Union member states.

That E.U. law requires companies and other organizations to minimize their collection and use of personal information. It also requires companies, schools and others to conduct audits, called Data Protection Impact Assessments, for certain practices, like processing sensitive personal information, that could pose high privacy risks.

But the Dutch central government and educational institutions have gone much further by commissioning exhaustive technical and legal assessments of complex software platforms like Microsoft Office and Google Workspace — and securing high-level company participation in the process.

“They have a centralized approach that leads to the ability to have scalable solutions,” said Julie Brill, the chief privacy officer at Microsoft. “The Netherlands punches above its weight.”



Julie Brill, Microsoft’s chief privacy officer, second from left, worked with the Dutch government on privacy issues. In 2018, she participated in a White House discussion on children’s use of the internet. Jonathan Ernst/Reuters

Last year, Zoom announced major changes to its data protection practices and policies after months of intensive discussions with SURF, a cooperative in the Netherlands that negotiates contracts with tech vendors on behalf of Dutch universities and research institutions.

Lynn Haaland, chief privacy officer at Zoom, said the talks had helped the video communications company understand how to improve its products to meet European data protection standards and “be more transparent with our users.”

Among other things, Zoom published an 11-page document detailing how the company collects and uses personal information about individuals participating in meetings and chats on its platform.

Dutch technical expertise has helped privacy auditors gain unusually granular insights into how some of the largest software companies amass personal data on hundreds of millions of people. It has also allowed Dutch experts to call out companies for practices that appear to violate European rules.

Some large American tech firms balk at first, said Sjoera Nas, a senior adviser at the Privacy Company, a consulting firm in The Hague that conducts the data risk assessments for the Dutch government and other institutions.

“We are so small that, initially, many cloud providers just look at us, raise an eyebrow and say: ‘So what? You’re the Netherlands. You don’t matter,’” said Ms. Nas, who helped lead the Dutch negotiations with Microsoft, Zoom and Google. But then, she said, the companies begin to understand that the Dutch teams are negotiating compliance for the Netherlands with data protection rules that also apply across the European Union.

“Then the tech providers realize that they won’t be able to supply their services to 450 million people,” Ms. Nas said.

The Dutch effort began to gather steam in 2018, after the country’s Ministry of Justice and Security commissioned an audit of an enterprise version of Microsoft Office. The report said Microsoft systematically collected up to 25,000 types of user activity like spelling changes and software performance details from programs like PowerPoint, Word and Outlook without providing documentation or giving administrators an option to limit that data gathering. In a blog post at the time, Ms. Nas, whose company conducted the audit, described the results as “alarming.”

Consumer software typically collects reams of usage and performance data from users’ devices and cloud services — diagnostic data that U.S. tech firms often freely employ for business purposes like developing new services. But under the E.U. law, diagnostic data tied to an identifiable user is considered personal information, just like the emails a person sends or the photos they post.

That means companies must limit their use of diagnostic personal data and provide people with copies of it upon request. The Dutch audit found Microsoft had failed to do so.

Microsoft agreed to address those issues. In 2019, the company introduced a new privacy and transparency policy for cloud customers worldwide that included “changes requested by the Dutch” Ministry of Justice, Ms. Brill wrote in a company blog post. Microsoft also released a data viewer tool to allow customers to see the “raw diagnostic data” that Office sent to the company.

Ms. Brill said the discussions with the Dutch helped Microsoft embrace European views on data protection, a shift in business culture that she said was more significant than the software changes.

“It begins with culture and then making sure that cultural pivot shows up in our products and our software and most importantly, in the way we describe what we do to our customers,” Ms. Brill said.

The pandemic accelerated the Dutch effect on U.S. tech companies.

In 2021, the Dutch audit of Google’s tools for schools, now known as Google Workspace for Education, reported that the products lacked certain privacy controls, transparency and contractual limits around their use of personal data. The education tools included apps like Gmail and Google Classroom, an online learning hub.

Google ultimately agreed to Dutch requests to significantly narrow how the company could use the personal data collected by its education tools — something that U.S. regulators had not accomplished.

Among other things, Google agreed to limit how it used diagnostic data from its core education apps to just three fixed purposes, down from more than a dozen purposes. The three uses included providing services to customers and handling problems like security threats.

Google also agreed not to use the diagnostic data for purposes like market research, user profiling or data analytics. And it agreed to develop a tool for education customers to see their diagnostic data.



“We had to explain to Google that school boards have a duty of care,” said Job Vos, a data protection officer for SIVON, a Dutch schools cooperative that negotiates contracts with tech vendors. Melissa Schriek for The New York Times

“We had to explain to Google that school boards have a duty of care, and they have to be in control of students’ personal data,” said Job Vos, a data protection officer for SIVON, a Dutch cooperative that negotiates contracts with tech vendors on behalf of Dutch schools, who participated in the yearslong talks with Google. “It cannot be used for commercial purposes.”

In a recent interview, Phil Venables, the chief information security officer at Google Cloud, said Google regularly worked with regulators around the globe and did not view the discussions with the Dutch — or the resulting changes in Google’s data practices — as particularly noteworthy. He added that the company welcomed the technical sophistication of the Dutch efforts.

“We’ve been happy to work with the Dutch because they’ve been exacting on this,” Mr. Venables said, “and we’ve responded to that.”

Google agreed to deliver new privacy controls and transparency tools by the end of 2022. Ms. Nas and Mr. Vos said they were now testing Google’s proposed solutions, a process that could take months.

The Dutch efforts could provide privacy improvements for schools in the United States and elsewhere, many of which lack the in-house technical expertise to independently investigate how complex platforms like Google collect and use students’ data.

But Dutch privacy experts see their audit and negotiation process as part of a much larger effort by countries trying to assert their digital sovereignty in the face of American tech superpowers.

“We’re basically captured by the tech behemoths,” Ms. Nas said. “We’re starting to realize that the only way to deal with it is to negotiate our way into their compliance with European standards.”

Natasha Singer is a business reporter covering health technology, education technology and consumer privacy. @natashanyt