Dear IBM Clients and Ecosystem Partners,

The privacy and security of data has become even more critical over the past year as the pandemic forced many organizations to accelerate their planned digital transformations. At IBM, we have always been, and remain, firmly committed to the responsible stewardship of data entrusted to us by our clients. It is how we have earned the trust of society and businesses for more than a century. We recognize that trust is earned, in part, through transparency. So, I am pleased to share that for 2020, we have updated IBM's Law Enforcement Requests Transparency Report to account for the full scope of IBM's business activities. Additionally, we will now be publishing this report every six months instead of annually. This will help ensure our clients have the most current information on this important topic.

As you will see in this year's report, IBM receives very few law enforcement requests for data. As an enterprise technology company, our clients are primarily other companies and, as such, are typically the more appropriate parties to receive requests for their own data. As a result, it is extremely rare (only once in the last year) that IBM provides anything more than basic account contact information, enabling a requesting law enforcement agency to approach a client directly. And as you will see from our 2020 Report, it continues to be a fact that IBM has not provided overseas client data to any government agency under any surveillance program involving bulk collection of content or metadata.

We want to be transparent about inquiries we receive from law enforcement agencies regarding data and the steps we take to protect the integrity of their information. To that end, I am pleased to share the following highlights for the period from January 1 to December 31, 2020:

- IBM received a total of 81 law enforcement requests.
- In all but one case we provided nothing more than subscriber information that enabled the requestor to engage directly with the owner of the data in question. Otherwise, we provided no information at all.
- In only one instance did we provide data to an agency outside the United States, and this was done in full compliance with local law.

In an age when trust is at a premium, especially trust across borders, sharing this report is a way for IBM to demonstrate the steps we take across the full breadth of our global operations to protect client data.

Trust and transparency are key to realizing the full potential of the digital economy. That's why they are the hallmark of [principles](#) that have long guided our company, and why IBM is creating innovative, privacy-preserving technologies such as [confidential computing](#) and [homomorphic encryption](#) to help unlock the true potential of data while protecting the information that matters most to individuals and organizations.

As IBM's Chief Privacy Officer, my mission is to help IBM ensure that open, transparent and explainable privacy practices are built into everything we do. It is a mission we take very seriously, and I hope you will see reflected in this report the values and practices that are critical to distinguishing our company as one of the world's most trusted brands.

Christina Montgomery
IBM Chief Privacy Officer

LINKS

IBM Principles for Trust & Transparency
https://www.ibm.com/blogs/policy/trust-principles/

(2013) A Letter to Our Clients About Government Access to Data
https://www.ibm.com/blogs/think/2014/03/open-letter-data/

C. Montgomery LinkedIn Blog: privacy preserving tech to unlock the true potential of data
https://www.linkedin.com/pulse/privacy-preserving-tech-key-unlocking-true-potential-data-montgomery-1e/

IBM
2020 Law Enforcement Requests Transparency Report

For more than a century, IBM has earned the trust of our clients by responsibly managing their most valuable data, and we have worked to earn the trust of society by ushering powerful new technologies into the world responsibly and with clear purpose.

Trust is foundational to our company and how we engage with our clients. That trust is reflected in our business model - where IBM clients' data is their data, and their insights are their insights. Client data and the insights produced on IBM's cloud or from IBM's AI are owned by IBM's clients.   These core principles for handling client data and insights, and those for building trust in AI and emerging technologies are located here: https://www.ibm.com/blogs/policy/trust-principles/. IBM's commitments are longstanding, as highlighted in our letter to our clients about government access to data. In 2020 IBM integrated the commitments in the letter into IBM's standard contracts. Those contractual commitments are viewable in our Data Protection Agreement.

GOVERNMENT ACCESS TO DATA

IBM has not provided client data to any government agency under any surveillance program involving bulk collection of content or metadata.

Following the law, protecting client data
- In general, if a government wants access to data held by IBM on behalf of an enterprise client, we expect that government to deal directly with that client.
- We do not provide access to client data stored outside the lawful jurisdiction of any government requesting such data, unless the request is made through internationally recognized legal channels such as mutual legal assistance treaties (MLATs).
- If we receive a request for enterprise client data that does not follow processes in accordance with local law, we will take appropriate steps to challenge the request through judicial action or other means.
- If we receive a government request for enterprise client data that includes a gag order prohibiting us from notifying that client, we will take appropriate steps to challenge the gag order through judicial action or other means.
- We will continue to work closely with governments and clients to balance the protection of data with law enforcement's obligation to conduct lawful investigations of criminal activity.
- IBM supports measures to increase the transparency, oversight and appropriate judicial review of government requests for data, including modernized international agreements on legal assistance.

TYPES OF INFORMATION REQUESTED

IBM Account Information
Requests for account information concern basic subscriber contact information, such as name, email, business address, and IP address.

Client Data
Client data requests concern content of data that IBM processes, stores, or hosts on a client's behalf. We treat requests for client data seriously and act in accordance with the belief that the client is the sole owner of their data and is the proper party to interact with the requestor. These types of requests are extremely rare for IBM because we cater to other companies and organizations, so we deal mainly with busines data which is not generally the target of such requests.

For the period January 1, 2020 to December 31, 2020, IBM processed the following number of law enforcement requests:

Agency/Region	Requests Received	Fulfilled Request Type	
		Account Information	Client Data
United States (Federal)	42	41	0
United States (State)	17	16	0
Other Countries	22	21	1 (United Kingdom)

Disclaimers