FUTURE OF PRIVACY FORUM

Consumer Genetic Testing Companies & The Role of Transparency Reports in Revealing Government Requests for User Data

Katelyn Ringrose and Alissa Gutierrez

The Future of Privacy Forum

The Future of Privacy Forum (FPF) is a catalyst for privacy leadership and scholarship advancing responsible data practices in support of emerging technologies. FPF is based in Washington, DC, and includes an advisory board composed of leading figures from industry, law, and advocacy groups. The views herein do not necessarily reflect those of our supporters or our Advisory Board.

Authors

Katelyn Ringrose, Christopher Wolf Diversity Law Fellow, Future of Privacy Forum

Alissa Gutierrez, Policy Intern, Future of Privacy Forum

Acknowledgements

Future of Privacy Forum (FPF) would like to thank Stacey Gray, Senior Counsel at the Future of Privacy Forum; and Rachele Hendricks-Sturrup, Health Policy Counsel at the Future of Privacy Forum.

Consumer Genetic Testing Companies & The Role of Transparency Reports in Revealing Government Requests for User Data

Introduction

Transparency reports, regularly published reports that companies voluntarily publish regarding key data protection issues, are essential tools for building consumer trust and maintaining accountability. Such reports play a particularly valuable role in illuminating whether and how law enforcement agencies seek data from companies providing digital services, as well as how companies respond to government requests for information about consumers. Leading companies in various industries routinely publish transparency reports,[1] with 70 major global firms issuing annual reports. The consumer genetics industry is at the forefront of issuing regular, user-friendly transparency reports that shed light on how law enforcement seeks access to user data.

FPF's Privacy Best Practices for Consumer Genetic Testing Services were developed in 2018 in collaboration with stakeholders[2] — including leading consumer genetic and personal genomic testing companies, regulators, scientists, and other experts. The Best Practices acknowledge that government agencies may have legitimate reasons to request access to consumer genetic data from time to time, but require that companies only provide access to such information when required by law. Legal requirements typically ensure that requests are vetted by an independent judge, particularized, and supported by probable cause.

Now, two years after the publication of FPF's Best Practices, we examine how leading consumer genetic testing companies require valid legal process for the disclosure of consumer genetic information to the government, as well as how companies publish transparency reports around such disclosures on at least an annual basis. Transparency reports are helpful tools for companies seeking to provide transparency regarding issues of concern to consumers, including how companies use data, moderate online content,[3] promote diversity and inclusion, and honor individual consumer and civil rights. Although the first transparency reports were issued by global platforms, including telecom and communication companies, companies in other sectors that have been the subject of law enforcement or national security requests are increasingly exploring the practice of issuing annual reports.

[1] Isedua Oribhabor and Peter Micek, *The What, Why, and Who of Transparency Reporting,* Access Now, (April 2, 2020), Accessed July 16, 2020, *https://www.accessnow.org/the-what-why-and-who-of-transparency-reporting/.*

[2] In January 2019, Family Tree DNA revealed an agreement with the FBI that conflicts with FPF's Best Practices. FPF immediately removed Family Tree DNA as a supporter of the *Privacy Best Practices for Consumer Genetic Testing Services.*

[3] Transparency Report 2019, Reddit, https://www.redditinc.com/policies/transparency-report-2019, (Reddit issues an annual transparency report that not only provides users with information about the types of requests the company receives from third parties to remove content or disclose private user data, but also issues statistics about the type and breadth of content moderation.).

In this report, we analyze: 1) the history and current state of reporting government access requests; 2) the benefits and purposes behind transparency reporting in the context of genetic testing services; 3) the types of law enforcement requests issued to consumer genetics testing companies; as well as 4) key conclusions from FPF's analysis of transparency reports issued by leading consumer genetic testing companies. Key conclusions:

- **First,** our findings reveal that most of the law enforcement requests to consumer genetic testing companies seek non-genetic information — like credit card transaction data that can be used to investigate credit card misuse, fraud, and identity theft.
- **Second,** leading consumer genetic testing companies have received few law enforcement access requests overall; the volume of government requests is fairly stable over time;
- **Third,** of the small number of requests for genetic information that companies receive, few result in disclosure of genetic data—companies have declined to disclose data to the government in response to improper requests and fought overly broad requests in court.[4]
- **Fourth,** the approach of leading consumer genetic testing companies stands in contrast to those publicly available genealogy services that have taken a more cooperative approach to law enforcement access and/or have failed to adopt transparency reporting as a practice. However, even those publicly available genealogy services that have historically taken a cooperative approach to law enforcement access are becoming more cognizant of privacy concerns by, for example, adopting opt-in, rather than opt-out choices for consumers who are willing to share their genetic information with law enforcement.
- **Finally,** none of the leading companies we surveyed reported that they have received a National Security Letter or a request for information under the Foreign Intelligence Surveillance Act.

[4] Rebecca Falconer, Ancestry.com Refused Court Request to Give Police DNA Database Access, Feb. 4, 2020, Axios, https://www.axios.com/ancestry-dna-database-search-warrant-privacy-11274a55-89c9-4f90-bc00-a521bf9b76bb.html, (Ancestry.com received one request seeking access to Ancestry.com's DNA database through a search warrant. Ancestry.com challenged the warrant on jurisdictional grounds and did not provide any customer data in response.).

The History and Current State of Reporting Government Access Requests

The first major company to launch a transparency report was Google, which in 2010, publicly released information concerning government requests for user data and government requests to remove content. The report followed Google's dispute with the US Department of Justice, in which Google refused a DOJ request to turn over records of millions of users' search queries.[5] Since Google published that first report, 70 major companies worldwide have released transparency reports.[6]

U.S. companies lead the publication of transparency reports,[7] with more than 40 US Internet and telecommunications companies engaged in the practice.[8] This group includes large, global internet firms. Increasingly, smaller companies that process sensitive data (e.g. Trade me,[9] Twilio,[10] and Silent Circle[11]) have followed the lead of those first tech platforms. More companies publish reports each year.[12] Companies in various sectors can benefit from issuing annual transparency reports that provide clarity to consumers about processes which would otherwise be shielded from public view.[13]

The Benefits and Purposes Behind Transparency Reporting in the Genetic Context

Companies publish transparency reports for a variety of reasons. Often, companies with consumer relationships, particularly if handling highly sensitive data, seek to build greater trust and clarity around the number and nature of government requests they receive. Transparency efforts may also help to inform media reporting and better educate policymakers who are concerned about government access to data. Broadly speaking, voluntary transparency reporting as a form of self-regulation can also shape the scope of appropriate public disclosures to inform future regulatory efforts. In addition, various forms of transparency reporting are increasingly appearing as legal requirements in proposed privacy laws.[14]

---

[5] *Google Transparency Report,* (2019), https://transparencyreport.google.com/about?hl=en.

[6] Supra, see Isedua Oribhabor and Peter Micek.

[7] Supra, see Isedua Oribhabor and Peter Micek.

[8] Liz Woolery, Ryan Budish, and Kevin Bankston, *The Transparency Reporting Toolkit,* (2016), Accessed July 16, 2020, https://cyber.harvard.edu/sites/cyber.harvard.edu/files/Final_Transparency.pdf.

[9] *Trade Me,* (2019), https://www.trademe.co.nz/trust-safety/2019/08/29/transparency-report-2019/.

[10] *Twilio,* (July 1, 2019 - December 31), https://twilio-cms-prod.s3.amazonaws.com/documents/Twilio_Transparency_Report_2019_H2.pdf.

[11] *Credo Transparency Reports,* (Q4 2019), https:https://www.credomobile.com/transparency-previous-reports?//www.credomobile.com/transparency-previous-reports?

[12] Supra, note 3.

[13] Rob Pegoraro, The Atlantic, Sep. 29, 2019, https://www.theatlantic.com/technology/archive/2019/09/what-happened-transparency-reports/599035/.

[14] Cal. Civ. Code § 1798.100, (The California Consumer Privacy Act of 2018 (the CCPA), for example, requires businesses covered by the law to comply with specific transparency obligations, such as a online and readily available description of a consumer's rights; the categories of personal information the business has collected about the consumer; the business or commercial purpose of collecting or selling personal information; and the categories of third parties with whom the business shares personal information.)

The practice of transparency reporting within the consumer genetic context is particularly important due to the perception that genetic testing companies hold data that is likely to be of interest to law enforcement. Government genetic databases, like the FBI's CODIS, hold genetic information of over 14 million[15] "offender" profiles. A 2019 MIT Technology Review report notes that more than 26 million people have taken an at-home DNA test.[16] Leading consumer genetic testing companies in the United States hold user genetic information from millions of consumers; this genetic information, or portions of that information, can be incredibly sensitive. Genetic information holds a strong potential for reidentification, can reveal intimate details about an individual's health and heritage; and can identify biological family members. While the capacity of this information to aid in law enforcement investigations is great, the sensitivity and personal nature of genetic information cannot be understated.

Most consumer genetic testing companies require legal process before disclosing genetic information. Some publicly available genealogy databases, which often allow consumers to upload genetic profiles from other websites, take a more cooperative approach to law enforcement requests. Such public databases have led to the apprehension of serial killers, the identification of missing persons' remains, and solved mysteries around other high-profile cold cases.[17] This cooperative approach can yield benefits. However, consumer genetic testing companies' databases and labs were not designed or intended to be used by law enforcement and the businesses rely on consumer trust. As such, most consumer testing firms implement safeguards, including legal process requirements, to protect consumer information.

Transparency reports demonstrate a company's public commitment to uphold user privacy and the security of their databases, even as law enforcement agencies realize the amount and potential usefulness of the data that technology companies store.[18] Transparency reports focused on law enforcement access typically include a summary of the number of access requests that a company received, as well as the company's compliance rate with such requests.[19] Reporting these statistics gives consumers the option to monitor the companies they interact with and how those companies in turn interact with law enforcement and other government agencies.

Furthermore, transparency reporting gives prospective consumers an informed choice of whether to engage with companies that take different approaches to government access.[20] In the context of international data transfers and their restrictions under the European Union's data protection

[15] Codis, NDIS Statistics, *FBI's Genetic Database CODIS,* https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics#:~:text=CODIS's%20primary%20metric%2C%20the%20%22Investigation,in%20more%20than%20503%2C968%20investigations.

[16] Antonio Regalado, *More than 26 Million People Have Taken an at-home Ancestry Test,* (February 11, 2019), https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.

[17] Gina Kolata, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder,* The New York Times, (April 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html 19 News; Brittany Bivins, *DNA Doe Project Close to Identifying Woman Likely Killed By Confessed Ohio Serial Killer,* (May 28, 2019), https://www.cleveland19.com/2019/05/28/dna-doe-project-close-connecting-unidentified-victim-ohio-serial-killer/;Kristin Lam, *Cold Case Cracked? Alabama Police Charge Truck-driving Preacher with 1999 Killings,* (Mar. 18, 2019), https://www.usatoday.com/story/news/nation/2019/03/18/coley-mccraney-charged-1999-alabama-killings-dna-match/3206930002/.

[18] *Id.*

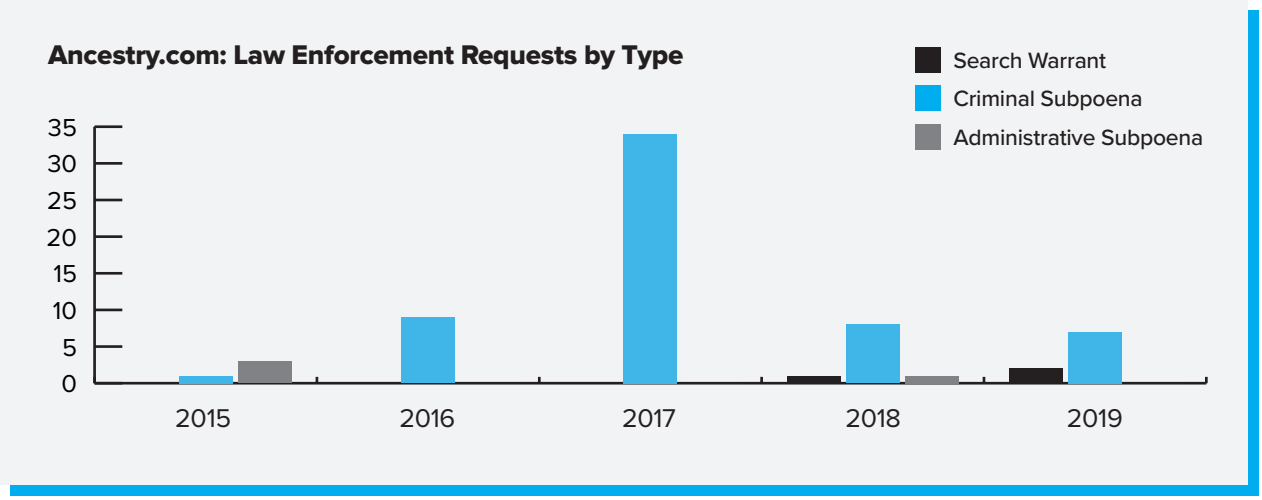
[19] See, New America, *Case Study #3: Transparency Reporting,* (last visited Jun. 15), 2020).https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/.

[20] *Id.*

law regime, transparency reports can be explored as a supplemental measure that supports international data flows, in addition to other safeguards, under Standard Contractual Clauses and alternative transfer mechanisms, where an adequacy decision of the European Commission is absent. At the very least, transparency reports can be used in the documentation process needed for international data transfers to indicate the level of risk of government access to data for different data flows.

Types of Law Enforcement Requests Issued to Consumer Genetic Testing Companies

Consumer genetic testing services generally require law enforcement, ranging from local police to federal agencies, to furnish them with a valid legal request — such as a **legal order, subpoena, judicial warrant, or national security letter (NSL),**[21] in order to retrieve consumer information. These requests are most often for non-genetic information (such as account records), or genetic information of an unknown person to be analyzed for identity or familial matches. Generally, biological samples are not submitted for a variety of practical and legal reasons.



The above chart shows the types of law enforcement requests that Ancestry.com received from 2015 - 2019.

[21] A national security letter (NSL) is a U.S. government-issued administrative subpoena to gather information for national security purposes.

Law enforcement requests can seek a variety of data types:

- **Non-genetic information.** As with other commercial sectors, law enforcement may request account records related to a particular name or credit card number, for example to investigate credit-card misuse, fraud, or identity theft. The mechanism for this kind of request typically involves a legal order[22] or subpoena.[23]
- **Genetic Information (DNA) of an Unknown Person.** In some cases, law enforcement requests involve DNA information of an unknown person, such as a suspected perpetrator of a crime. Federally-funded law enforcement must exhaust all other available agency-run databases, such as CODIS and similar state-run databases (SDIS), prior to turning to non-governmental databases.[24] If the identity of the person is not tied to a profile within a government-run database, a law enforcement request to a genetic testing company typically has two goals: 1) to identify the person, or 2) to identify close familial matches, such as immediate family or even distant relatives. In these cases, the mechanism for requesting that a consumer genetic company perform such a search is typically a warrant, requiring judicial approval and probable cause.[25]
- **Biological Samples.** In general, biological samples (such as blood or saliva) are not practical to submit to non-government databases, and involve a variety of legal obstacles. For example, consumer genetic testing companies test saliva, not other material containing DNA. Furthermore, evidentiary and chain of custody issues around biological samples often require samples to be processed in CODIS-approved laboratories. Department of Justice guidelines prohibit federally-funded law enforcement entities from submitting biological samples or genetic information under a pseudonym.[26] If a law enforcement officer were to submit a suspect's DNA samples, they would be in violation of companies' Terms of Service, which typically require customers to submit only their own biological samples.

[22] A legal order is a formal request issued by a court of law requiring that an online platform disclose user information information.

[23] A subpoena is a request for the production of documents, or a request to appear in court or other legal proceeding. A subpoena issued in a criminal case may be requested by opposing counsel, and must be approved by a judge, magistrate, or clerk.

[24] United States Department Of Justice, *Interim Policy Forensic Genetic Genealogical Dna Analysis And Searching* (Accessed July 15, 2020), https://www.justice.gov/olp/page/file/1204386/download; Katelyn Ringrose, DOJ Doesn't go far Enough to Limit Searches of Consumer DNA Services, The Hill, (October 4, 2019) Accessed July 15, 2020, https://thehill.com/opinion/technology/463835-doj-doesnt-go-far-enough-to-limit-searches-of-consumer-dna-services.

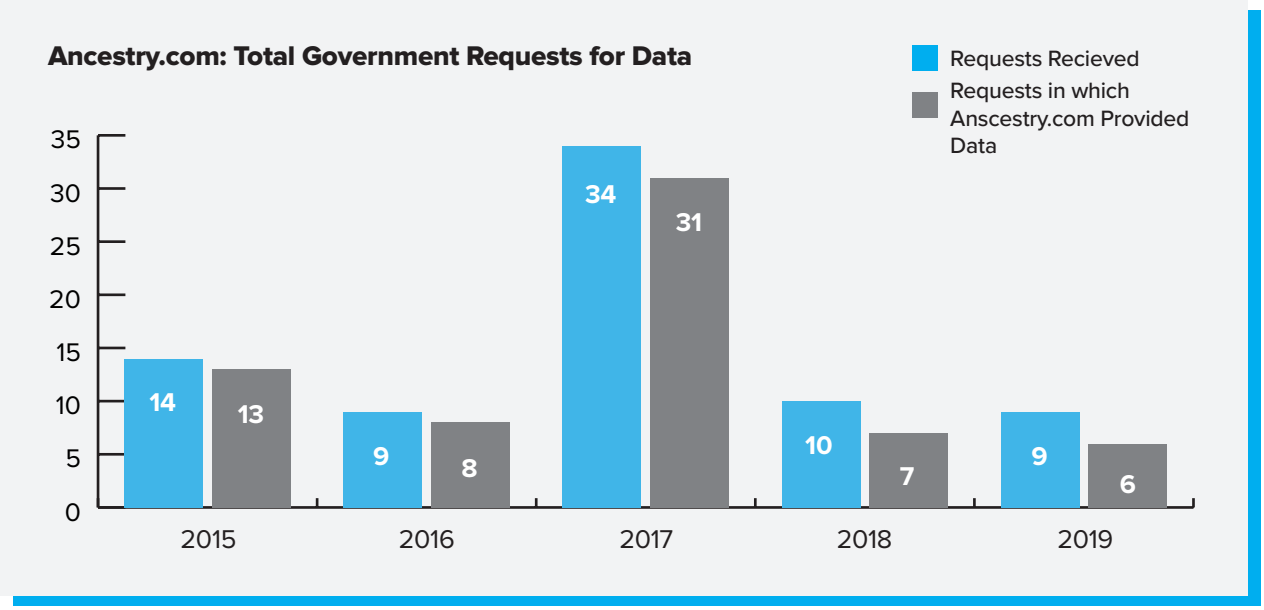
[25] *23andMe Guide for Law Enforcement,* 23andMe, https://bit.ly/3eC72Fk.

[26] United States Department Of Justice, *Interim Policy Forensic Genetic Genealogical Dna Analysis And Searching* (Accessed July 15, 2020), https://www.justice.gov/olp/page/file/1204386/download.

Highlights From Transparency Reports of Leading Consumer Genetic Testing Companies

A number of consumer genetic companies issue transparency reports, include information regarding law enforcement access with their privacy policies, and have reported to the media regarding how often they receive law enforcement requests. Ancestry.com and 23andMe have emerged as leading companies, with both issuing regular, extensive reports. Both Ancestry.com and 23andMe have reported information pertaining to the number of law access requests and national security letters received, as well as the number of requests each company honored.

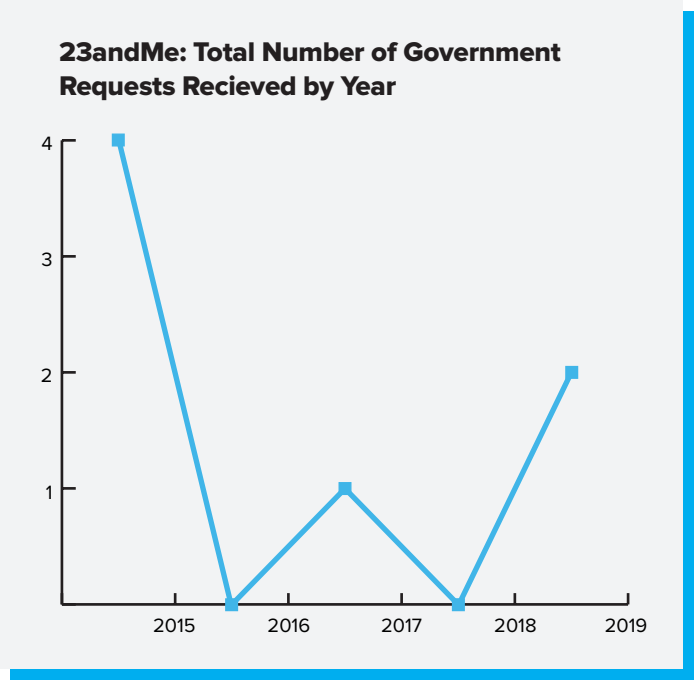
Analyzing transparency reports from these two companies, we observe that: 1) the overwhelming majority of requests are for account or non-genetic information; 2) trends around how many access requests companies receive have remained relatively stable over time; 3) of the relatively few warrants issued for genetic information, many have been refused and/or litigated; 4) publicly available genealogy databases may be becoming more privacy-centric over time as well; and finally 5) no companies that support the Privacy Best Practices for Consumer Genetic Testing Services report receiving any National Security Letters.



This chart differentiates between the requests received by Ancestry.com, and the requests the company fulfilled.

Transparency reports issued by genetic testing companies generally include the number of requests received; the scope of those requests; and how and when they comply with those requests. According to Ancestry.com and 23andMe, the overwhelming majority of requests are for account or non-genetic information. This is probably not surprising given the prevalence of these kinds of requests across other sectors.

For example, Google reports that over the course of 2019, the company has received more than 340,000 government requests for account-related data globally.[27] In contrast, neither Ancestry.com and 23andMe have ever received more than 34 access requests in a year.[28] While full 2020 statistics won't be available until the end of the year, Ancestry.com recently issued the company's biannual update to its transparency report—the update identifies three requests for account-level information via criminal subpoena for investigations involving credit card fraud, credit card misuse, or identity theft from January 2020 to June 2020. Out of these three requests for information, Ancestry.com provided information in one instance.[29]



In addition to receiving relatively few access requests, trends around how many access requests companies receive have remained relatively stable over time. While one may expect to see more law enforcement attempts to access genetic information pursuant to media coverage of the high profile cold case killers, according to Ancestry.com and 23andMe law enforcement requests for both account-related information and genetic information haven't increased over time.

Despite media perceptions of law enforcement access to genetic data, warrants requesting genetic data are relatively few. Of the relatively few warrants issued to Ancestry.com and 23andMe for genetic information, many have been refused and/or litigated for being overly broad. The Fourth Amendment to the US Constitution prohibits unreasonable searches and seizures, requiring that warrants be: issued by a judge or magistrate, justified by probable cause, and supported by an oath or affirmation. A warrant must also describe the place to be searched and the persons or things to be seized with particularity. Therefore, a warrant issued to a consumer genetic company must

[27] Google Transparency Report, *Government Request to Remove Content,* (June 2020), https://transparencyreport.google.com/government-removals/overview.

[28] In 2017, Ancestry.com reported receiving 34 law enforcement requests for user data; the vast majority of those requests were for non-genetic user information.https://www.ancestry.com/cs/transparency-2017.

[29] *Ancestry Transparency Report,* July 2020, https://www.ancestry.com/cs/transparency.

describe what the law enforcement officer/agency is seeking with some degree of particularity.[30] While this is an evolving area of law, warrants that ask consumer genetic testing companies to investigate their databases for familial matches and partial matches of DNA could all be deemed overly broad. In the genetic testing space, consumer trust is important and fighting overly broad or improperly served warrants is one way that companies can uphold consumer trust. As of June 2020, Ancestry.com received two warrants seeking access to the company's genetic database within the previous six months. Ancestry.com challenged both requests—one was withdrawn and the other remains unresolved.

In past years, some publicly available genealogy databases took a cooperative approach to law enforcement requests for genetic data. Recently, some public databases have adopted a more privacy-centric approach. Publicly available genealogy database GEDmatch, which previously took a more cooperative approach toward law enforcement requests, recently announced an opt-in program in 2019, whereby users could choose to share their genetic information for a variety of purposes. Following that announcement, less than 20% of users[31] chose to opt into sharing their genetic information with law enforcement.[32]

No companies that support the Privacy Best Practices for Consumer Genetic Testing Services report receiving National Security Letters. While companies can report the specific number of warrants, subpoenas, or legal order they receive, the United States government limits how companies can report the number of National Security Letters they receive.[33] For companies that receive less than 1,000 National Security Letters, Department of Justice regulations only allow companies to disclose that they have received anywhere from 0 to 1,000 requests.[34] National Security Letters are most often issued by federal agencies during counterterrorism and counterintelligence investigations—the consumer genetic testing companies reports of receiving zero National Security Letters align with analyses suggesting that these types of requests are most often received by firms in the telecommunications and banking sectors, as well as Internet Service Providers.[35]

[30] *Maryland v. King,* 569 U.S. 435 (an arrestee's DNA can be taken as part of a regular booking procedure under the Fourth Amendment, the case does not mention consumer genetic testing services or publicly available genealogy databases); *Carpenter v. United States,* No. 16-402, 585 U.S. _____, at 3, (explores the issue of the third-party doctrine in relation to cell-site location information, touches briefly on genetic privacy in Gorsuch's dissent, "Can [the government] secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of Katz. But that result strikes most lawyers and judges today—me included—as pretty unlikely.')

[31] Just 185,000 of the site's 1.3 million users chose to opt in to sharing their genetic information with law enforcement.

[32] Kashmir Hill and Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise,* (Nov. 5, 2019), updated Dec. 30, 2019, https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html.

[33] See Twitter v. Barr, EFF Amicus Brief,https://www.eff.org/document/amicus-brief-26.

[34] *Id.*

[35] "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies," Jennifer Valentino-DeVries, Sept. 20, 2019 (detailing NSLs issued to "credit agencies, financial institutions, cellphone carriers, and tech giants.") https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html; See also, National Security Letters: FAQ, EFF.org, https://www.eff.org/issues/national-security-letters/faq#:~:text=A%20national%20security%20letter%20(NSL,of%20national%20security%2Drelated%20investigations.

Conclusion

The rapid growth of technology platforms and online services calls for greater accountability, transparency, and enhanced consumer rights. Transparency reporting provides a clear process in which leading companies can build and maintain trust with their consumers. Transparency reporting enables consumer genetic testing companies to promote visibility about law enforcement requests, provide consumers with information about government uses of data, and disclose threats to consumers' privacy. Companies in other sectors that process sensitive user information should follow the lead of consumer genetic testing companies by issuing annual, clear, and consumer-friendly transparency reporting outlining their approach to law enforcement access requests.


FUTURE OF
PRIVACY
FORUM