@PrivacyandDataProtection

# Q4 2021 Privacy & Data Protection Report

As previewed in the EOY Board Report, this report provides an overview of the 2021 progress on the top PDP Risks and a preview of the top 2022 PDP Risks.

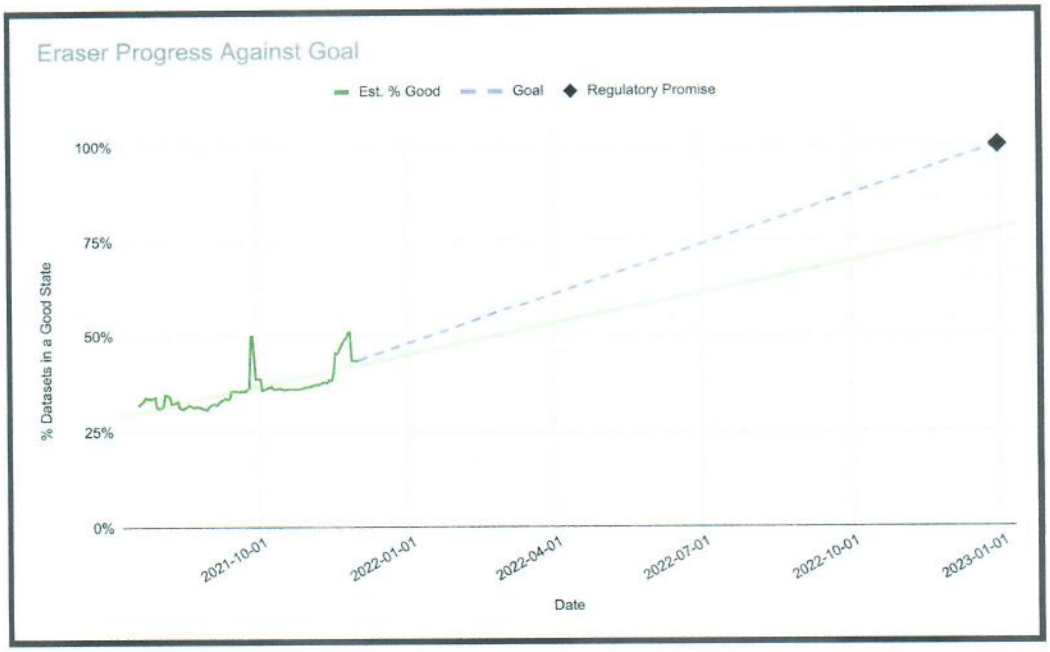
## 2021 Top Risks Review

### Data Hygiene

One of our highest risks has long been our inability to know what data we have, who has access to it, who/what is using it, can we delete the data if asked, and how long are we keeping the data for. Together these can largely be summarized as data hygiene risks. While this presents a set of significant risks grouped together, the two that have been a primary focus in 2021 are Data Deletion and Access Controls.

**Data Deletion**

Over the last two quarters we have seen progress in our deletion efforts. Below shows the percentage of data that is in a good state (i.e., we know what it is, where it is, and are capable of deleting it as needed) against data that has yet to be brought into a good state (i.e., we don't know what it is, where it is, what it's used for, and we don't delete it).



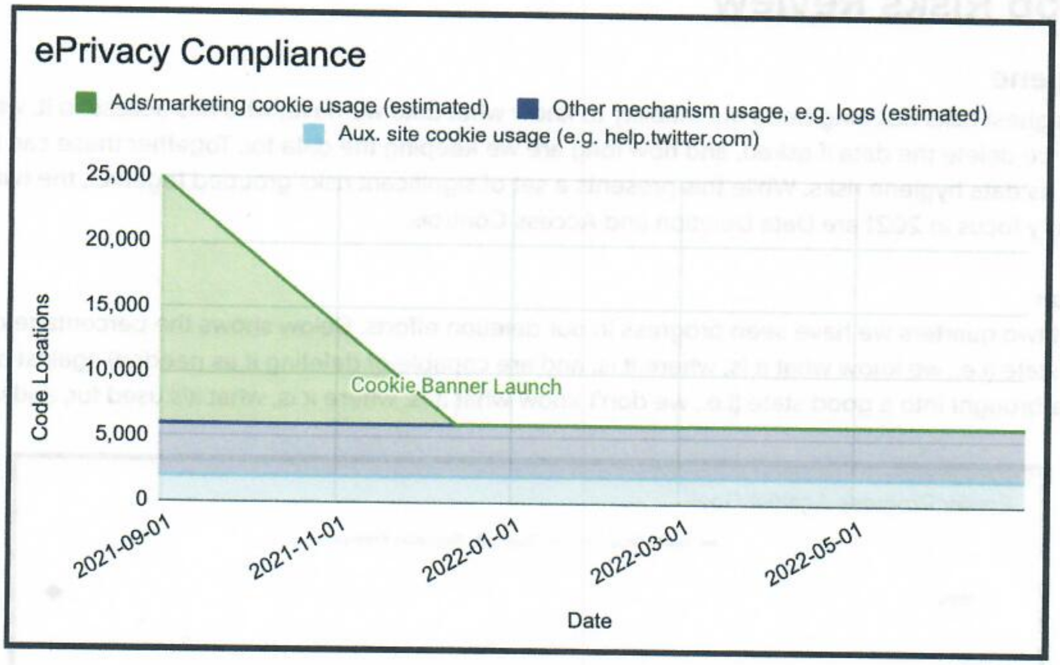
Progress is significantly slower than hoped and without consistent sustained prioritization and additional resources, we are not likely to hit our Q4 2022 deadline.

**Access Controls**

Excessive (i.e., access that is not needed to perform one's function) access to data remains a significant risk. Work has slowly progressed to create some roles-based access measures but these are not where they need to be. Every new employee has access to data they do not need to have access to for the purpose of their role. Until we have implemented a mature centrally owned and operated system to manage access to data (e.g., entitlements and review, Role Based Access Controls, audits, etc) we are at risk of inappropriate access or use of data. Our inability to delete data compounds that risk, as we retain data that we should not have and which is therefore accessible by people who do not need to have access to this data.

### Cookies

We have made significant progress on work to bring our usage of cookies up to the appropriate standard. In December 2021 we will launch an updated cookie banner in France which will correctly separate out and respect a person's choice between essential and non-essential cookies in France (depicted below are the relevant data uses of cookie related data collected from Twitter web properties against the timeline for remediation). All things going well, we expect to roll this banner out across the EU and UK in early January 2022.



### FTC Settlement Preparations

During 2021 we made significant progress in preparing to meet our obligations under the new FTC Consent Order. We have prepared runbooks for all of the required aspects of the Consent Order; engaged a third party to conduct work to collect all public statements to prepare a questionnaire for teams to ensure their products and services match our public statements; we have audited existing security and privacy controls, identified missing controls, and begun the process of establishing new control owners; we have begun preparing Flyway (our SDLC) to meet the requirements that all security and privacy reviews are conducted as needed; we have prepared trainings (not yet administered) for teams; and we have begun internal communications to teams about the FTC Consent Order. Progress in some areas was slower than hoped. For example, we had hoped that teams would have completed their review of the questionnaire regarding public statements by year end, however, the questionnaire has required additional time to finalize.

## 2022 Top Risks Preview

### Data Hygiene

We will need to extend our work beyond deletion and access controls to properly mitigate our risks with respect to data hygiene more generally. This work is exceptionally cross-functional and requires support and commitments from teams across the company to achieve our data hygiene needs.

### Data Deletion and Usage

While we have set a Q4 2022 deadline for ourselves following conversations with the Irish Data Protection authority, if this risk becomes publicly known or the subject of a focused investigation while we are still fixing this issue, the risk to Twitter will be significant.

### Access Controls

Addressing the state of access controls at Twitter will continue to present significant challenges in two respects: 1) creating access controls, as much data still has no controls 2) using them consistently and effectively to control access to data.

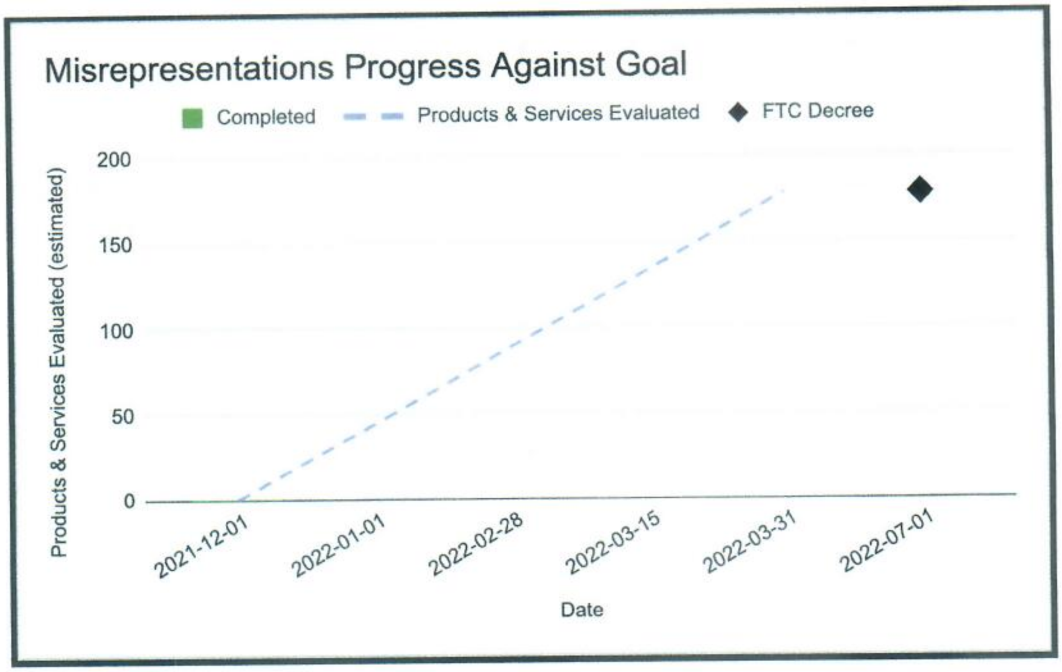
## Cookies

Despite our efforts to date, we expect to continue to face regulatory investigations for our use of cookie technology. These investigations will focus on both historical cookie usage and how we are using cookie technology under the new banner. We are likely to face monetary penalties and be ordered to make changes to how we're using cookie technology for advertising, analytics, and keeping people logged into Twitter for prolonged periods of time going forward

## FTC Settlement Preparations

In addition to ensuring the respective PDP and Security Programs are sufficient, there is additional work underway to meet specific obligations under the FTC Consent Order. These include ensuring:

- **Existing Products, Services, and Systems Operate Consistent with Existing Security and Privacy Statements:** We collected 5 years worth of statements (i.e., >20K statements), analyzed them into categories of representations, and created a questionnaire that teams that own Products, Services, or Systems can assess whether their Products, Services, or Systems are operating consistently with our existing statements. We will need all impacted teams (i.e., >180 services/products) to complete the questionnaire, identify any gaps, and propose remediation steps during Q1 2022 (depicted below).



- **Data Deletion Occurs:** We must deliver on our promises around data deletion. This work has been ongoing for many years and while progress has recently been made, it is insufficiently fast to meet our Q4 2022 target. We intend to build and lean more on infrastructure which enforces deletion to reach this goal.
- **Ensuring that Emails and Phone Numbers Collected Through Security Flows are Not Used in Advertising Products**: Technical means are beginning to roll out to ensure that we do not misuse emails and phone numbers. Until those are in place, we are still relying on fragile infrastructure and processes to prevent a recurrence of our prior misuse. Delivering technical solutions in 2022 will be key to long term compliance with our obligations.

## Privacy and Security Programs

To meet our FTC Consent Order obligations we must have a Security Program and a Privacy Program that are capable of protecting the privacy, security, confidentiality and integrity of data Twitter has. Based on our work with our external partners over the last year, we know that our programs are less mature than they should be. This will present a heightened risk as under the new FTC Consent Order, these programs will be subject to additional audit scrutiny. Ensuring the programs are appropriately mature will be key to mitigating our risk.

### PDP Program

The updated Program will be key to meeting our FTC Consent Order obligations. Based on progress so far, we will need cross functional support to:

- **Operationalize the Data Governance Committee (DGC)**: as decisions related to data collection, use, maintenance, access and sharing are raised we will need to ensure that the DGC have oversight over these decisions.
- **Implement New Controls (i.e., taken from ISO frameworks) Ensure Ownership and Effective Operation**: in consultation with third-party auditors we have identified a significant number of controls that will need to be implemented across the company.
- **Ensure Required Reviews (Security and Privacy) Facilitated Through Flyway are Completed**: Flyway V2 is launching, which will provide the easiest auditable way of assessing whether appropriate reviews have been completed. Ensuring teams use Flyway will provide us the strongest way to ensure the appropriate reviews are being carried out.
- **Update Policies and Procedures and Enforce Them**: Policies and operational runbooks related to data that have been updated are neomg adhered to.
- **Ensure Required PDP Trainings are Completed**: these will be recurrent trainings and vary based on an employee's role and responsibilities
- **Operationalize Reviews and Audit Trails for Public Statements Related to Privacy or Security**: we must have a process in place to ensure that any statement that we make to the public related to privacy and security is reviewed, and logged as having been reviewed.

[redacted]