III. PARTICIPANT PROFILES

A. BP P.L.C.

1. Background

BP P.L.C., registered in England and Wales, is one of the world's leading international oil and gas companies. It provides customers worldwide with fuel for transportation, energy for heat and light, lubricants to keep engines moving, and the petrochemicals products used to make everyday items as diverse as paints, clothes, and packaging. BP has 84,500 employees in nearly 80 countries, about 17,200 retail sites, and it generates economic value of $359.8 billion. ACC had an opportunity to speak with Ellis Parry, BP's Global Lead—Data Privacy. Parry's role focuses on global privacy issues management – data security being a distinct but closely aligned discipline at BP as it is in many conglomerates.

Parry is a contributing author to Sweet & Maxwell's "Data Protection Law and Practice" (4th ed.), IAPP's "Building a Privacy Program," and Nymity's "A Privacy Office Guide to Demonstrating Accountability."

2. Organizational Structure of the Privacy Group

BP is a large organization that is mature and sophisticated in its management of personal data. Personal information is managed according to BP's "Binding Corporate Rules," which is a global compliance framework forged from the European concept of data privacy. BP's rules meet 28 separate European member states' standards for data privacy, which all 100% owned BP entities, irrespective of where they are located in the world, must operationalize.

For instance, when someone applies for a job with BP anywhere in the world, Parry explains, the global data privacy policy sets out how information should be collected from the applicant so that it meets European Union standards as embodied by BP's BCR framework. So, an applicant in Germany (as an example of a country with some of the strictest data privacy laws in the world) should have the same experience as someone who applies in Oman or another country with less stringent requirements. The Binding Corporate Rules ensure that BP's data privacy handling standards are uniform across the global organisation. BP was one of the first multinational companies to adopt this European model as a global standard.

The data privacy policy and personal information handling standards are standardized worldwide, with local versions where necessary that may set out a specialized policy or process for a particular area, such as consumer marketing or a given business line. The variations deal with specific scenarios when local laws exceed BP's global standards.

In terms of staffing, there is a central data privacy team, the members of which are located globally. The central team members are responsible for specific areas of the world, such as Asia Pacific, Western Hemisphere, Northern and Southern Europe. In countries where BP has a wholly owned legal entity that employs at least twenty or more staff, BP appoints a local privacy coordinator who is responsible for the privacy program roll-out locally. That person reports locally, but the central team liaises with them closely offering active support and advice. The LPC role takes about ten to fifteen percent of the person's time, so the job is often taken on by the Human Resources Manager or a local IT or Legal staff member.

Joint ventures' policies depend on which entity has majority ownership. BP seeks to apply its policy when it has majority ownership; otherwise, it encourages the joint venture partner to accept its privacy policy and practices.

3. Key Elements of the BP Privacy and Data Protection Program

When an incident arises, the organization's preparedness is key to managing it successfully, Parry says. A company should have its written procedures readily available. People need to understand the process—both staff and stakeholders. Within BP, there are mandated reporters who must relay privacy breaches that come to their attention, although every staff member is responsible for alerting the correct stakeholders to issues which raise concerns. The incident response process includes the following steps:

- Breach
- Containment
- Preliminary Assessment
- Evaluation of Risk
- Notification (external regulators and/or affected individuals as needed)
- Future Prevention

Everything proceeds on a very tight time schedule. Teams need to understand their roles in advance, which is helped by performing dry runs.

For vendor facing programs, the vendors are triaged into segments according to the size of the BP spend and the sensitivity of the data the vendor handles. In contractual negotiations BP seeks to align vendor privacy programs with the company's own global program. The Central Data Privacy Team sets the strategy, produces the tools, and then supports the various business units' implementation of the centrally mandated strategy.

With regard to BYOD, if employees need a mobile device to perform their job role then BP will give them one, but BYOD is possible for most workers. For some teams, however, BYOD is not allowed owing to the sensitivity of the information they handle. In terms of technology, BP information on BYOD devices resides inside a virtual encrypted data "container" within the BYOD device. It is impossible to access a BP-provided email account on a BYOD device without first installing an app, which is available internally from the BP app store. It is a high-security third-party solution in its second generation. If the user loses the device, BP sends a

kill message to the lost mobile device, but BP is confident that the local encryption on the missing device ensures an adequate level of data protection even if the kill switch is not successfully activated.

4. Global Data Compliance

According to Parry, European regulators are frustrated with their inability to control large Internet companies without European headquarters. The apex of this battle is the European Court of Justice's "right to be forgotten" case allowing people, under certain circumstances, to rewrite their discoverable on-line history by demanding search engines de-list results which are returned when their personal information has been used as the search term. These types of decisions will have a dramatic impact on how search engine providers operate, raising new challenges and issues, Parry says, including an ideological battle between champions of freedom of expression and privacy advocates.

5. Leading Practices

When considering success factors for privacy programs, first take care in deciding what you measure, Parry advises. There is no legal or regulatory necessity yet to measure a program's success. BP gauges the success of its privacy program locally, then aggregates that data so that BP can demonstrate successful roll-outs by country or region or for BP as a whole across the globe. This system of measurement allows the Central Data Privacy Team to find potential gaps that indicate areas for focus in the short to medium term.