Organizational Accountability in Light of FTC Consent Orders

Paper Snapshot

- **Privacy management and compliance programs must be considered in light of FTC consent orders.**
- **Recent FTC settlements with Facebook and Equifax reaffirmed and provided further information on the FTC's expectations of what such programs need to include.**
- **The privacy program requirements outlined in the recent FTC settlements address all elements of organizational accountability (i.e. leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement).**
- **Every company is responsible for identifying relevant measures to effectuate these elements through privacy management and compliance programs based on the nature of their business, size of company, extent of data processing, etc.**
- **FTC consent orders have precedential value for future investigations and are instructive to all organizations, but it is important to remember that some granular requirements may be specific only to the company that is the subject of the order.**

I. Introduction

In the United States, organizational accountability is a requirement that has long been established in law and regulatory guidance across a wide variety of corporate compliance areas.[1] In the US privacy realm, the Federal Trade Commission (FTC) has traditionally spelled out many of accountability's key features through its consent decrees. Practically every consent decree resulting from an FTC privacy case has included a requirement to establish and implement a written privacy and security program, with many of these incorporating the essential elements of organizational accountability, as discussed below.[2]

Nevertheless, over the past year, we have seen an increasing focus on corporate accountability in privacy in the US. Members of Congress are exploring organizational accountability in connection with a new US federal privacy law and state legislators are including various elements of accountability in state privacy bills. Examples of such elements include a risk-based approach to privacy and data management, and oversight requirements. Most importantly, and the subject of this paper, are the recent transformative changes to FTC consent decrees which serve as clear indications of the Commission's focus on organizational accountability as a means to achieving and demonstrating compliance.

These transformative changes are relevant to all companies because:

1. FTC consent orders have precedential value beyond the target of an investigation.

2. The requirements imposed by the FTC via its consent orders constitute what it believes is necessary for the company in question to achieve compliance with relevant legal obligations and provide guidance for other companies on best practices.

Recent FTC consent orders have become much more detailed than those of prior enforcement actions.[3] They indicate, in many ways, an even greater emphasis than before on organizations having comprehensive internal processes and programs in place to ensure compliance with relevant legal requirements. While the specifics of the programs outlined in FTC consent orders reflect the particular data use practices and compliance history of the organization subject to the order, the underlying requirement to implement a comprehensive privacy program, and even some of the specific requirements for such programs, should be seen as instructive to all businesses that collect, use and share personal data. Indeed, this is inherent in the FTC's enforcement model, which is to select and prioritize cases that have precedential value beyond the immediate target of the investigation. Thus, it is fair to say that FTC consent orders may be an indication of the possible standard against which all companies may be measured going forward.

This paper will explore the recent $5 billion dollar FTC settlement with Facebook ("Facebook Settlement") which resulted from Facebook's alleged violation of a prior 2012 FTC consent order.[4] It will also examine the recent FTC settlement with Equifax, related to its 2017 data breach ("Equifax Settlement").[5]

While many aspects of these settlements reflect familiar features of organizational accountability in data privacy, they also introduce several requirements that are both uniquely rigorous and detailed and that impose new types of obligations that are not commonly reflected in most privacy accountability programs. From one perspective, both settlements are very much in line with global approaches to organizational accountability, including some of the elements of accountability codified in the EU General Data Protection Regulation (GDPR),[6] regulatory guidance on organizational accountability from global regulators[7] and the accountability "indicators" put forward in a 2018 sweep on "privacy accountability" by the Global Privacy Enforcement Network (GPEN).[8] From another perspective, however, the settlements elevate privacy accountability to the level of financial controls (e.g. increased use of certifications and multiple lines of oversight). In this way, these settlements will likely result in a step change in organizational focus on, and investment in, privacy accountability.

II. Essential Elements of Accountability

The requirements of the Facebook and Equifax settlements are consistent with the essential elements of accountability that the Centre for Information Policy Leadership (CIPL)[9] has promoted for many years.[10] These elements include leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement.

Figure 1 – CIPL "Accountability Wheel" – Universal Elements of Accountability

Implementing these elements involves:

- **Establishing leadership and oversight for data protection and the responsible use of data**, including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's accountability program and report to management and the board;

- **Assessing and mitigating the risks** that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means

conducting periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology and other factors and adapting the program to changing levels of risk;

- **Establishing internal written policies and procedures** that operationalize legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards as well as the organization's values and goals;

- **Providing transparency to all stakeholders internally and externally** about the organization's data privacy program, procedures and protections, data uses, the rights of individuals in relation to their data and the benefits and/or potential risks of data processing. This may also include communicating with relevant data privacy authorities, business partners and third parties about the organization's privacy program;

- **Providing training for employees and raising awareness** of the internal privacy program, its objectives and requirements, and implementation of its requirements in line with the employees' roles and job responsibilities, as well as of the importance of privacy and data protection in general. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility;

- **Monitoring and verifying the implementation and effectiveness of the program and internal compliance** with the overall privacy program, policies, procedures and controls through regular internal or external audits, other monitoring mechanisms and redress plans; and

- **Implementing response and enforcement procedures** to address inquiries, complaints, data protection breaches and internal non-compliance, and to enforce against acts of non-compliance.

In addition to being in line with the essential elements of accountability, many of the requirements of the Facebook and Equifax settlements reflect an increased focus on specific accountability requirements and reaffirm their importance as part of accountable privacy and security programs.

For example, the FTC began its investigation of Facebook following alleged misuse of data by Cambridge Analytica, a third party that had received information in violation of Facebook's rules. The Facebook Settlement adopts specific obligations for Facebook to actively oversee the activities of its data recipients. Arguably, due diligence in data sharing initiatives or with third party business partners forms part of accountability under the elements of policies and procedures and monitoring and verification. However, the FTC has now reaffirmed such a requirement, perhaps even going beyond the level at which such due diligence traditionally takes place in companies today.

The FTC also reaffirms obligations around risk monitoring, testing and incident detection and disclosure in both the Facebook and Equifax settlements. Many companies have, to date, implemented incident detection procedures, including 24/7 corporate wide incident reporting lines, as well as incident response, prevention and reporting systems. Both settlements indicate that while some companies have traditionally put an increased focus on such measures, now every organization will be expected to implement such controls as part of their accountable privacy and security programs. Furthermore, the Equifax Settlement demonstrates, in particular, that information security programs are subject to the

same standard of accountability as those of privacy programs. This makes sense considering that such information security programs will need to work in parallel or in tandem with such privacy programs.

Finally, the FTC reflects, in the Facebook Settlement, that not only procedural but also technical controls will be needed to ensure that policy decisions made about data processing are honored consistently across the organization. While the Facebook Settlement gives the company discretion in how it implements these compliance obligations, the company's accountability program will likely reflect an unprecedented technical investment around privacy. There is likely to be an increased emphasis on ensuring compliance with legal requirements and policy decisions via procedural, contractual and technical controls in FTC consent orders going forward.

The following sections demonstrate that the requirements of both settlements map to the essential elements of accountability. In the case of the Facebook Settlement, the following section also includes a table comparing the order requirements with data privacy obligations mandated under the GDPR.[11]

Note that the mapping charts and table in the following sections should not be construed as legal advice or as representing the views of any individual CIPL member company or the law firm of Hunton Andrews Kurth. In comparing the requirements of the settlements with the essential elements of accountability and comparing the Facebook settlement obligations with requirements imposed by the GDPR, CIPL exercised a degree of interpretation and judgment.

III. Facebook Settlement Requirements Mapped to the Elements of Organizational Accountability

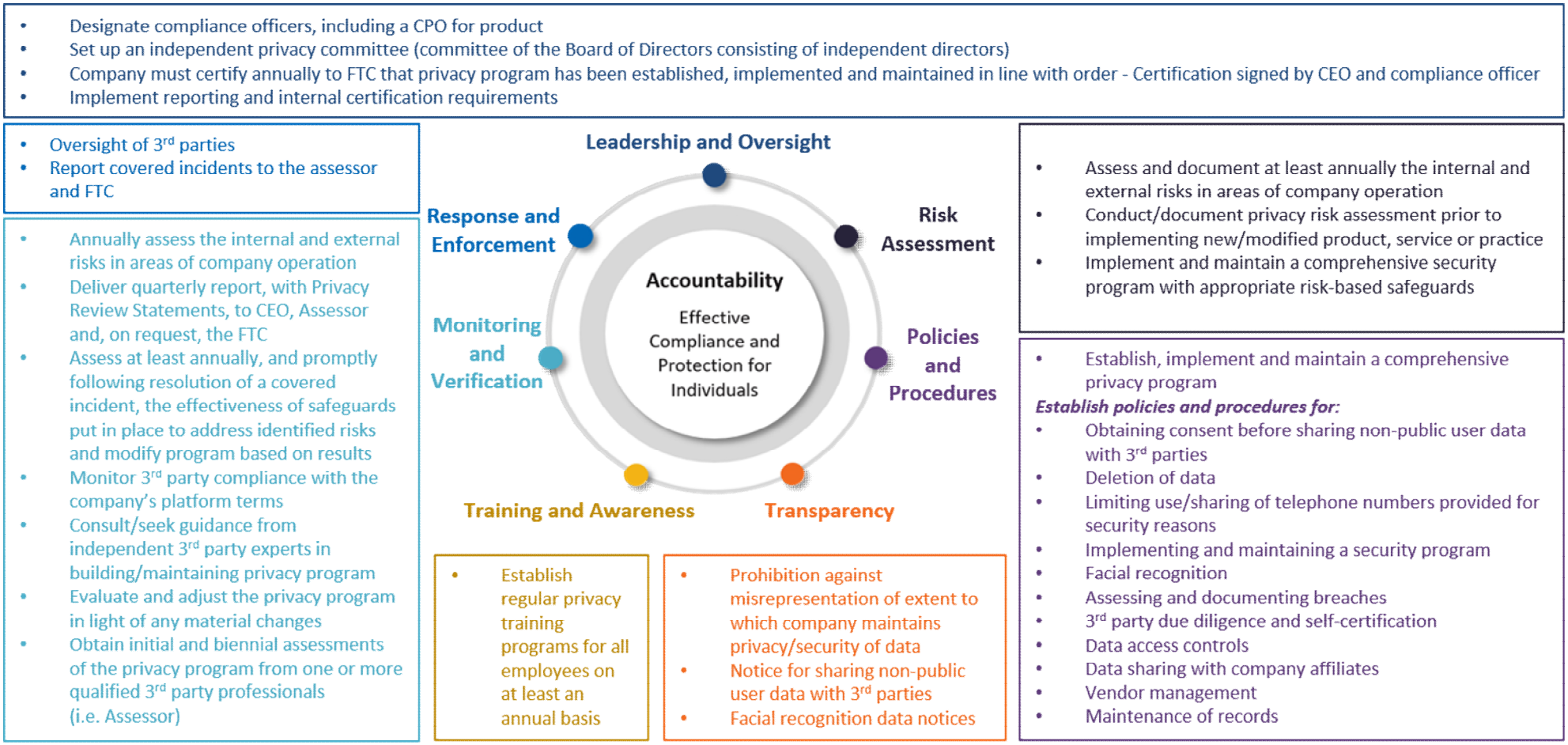

Figure 2 – Facebook Settlement Requirements Mapped to CIPL "Accountability Wheel"

* Note: Some of these controls may be relevant to more than one accountability element.

Detailed Mapping of the Facebook Settlement Requirements to the Elements of Accountability and Comparative Analysis against EU GDPR Requirements

The following table outlines, in detail, Facebook's obligations under the settlement. The table also compares these obligations with the obligations imposed on controllers and processors under the GDPR. This table is comparative in nature only and comments strictly on the extent to which the accountability requirements map to those required by the GDPR.

- **Aligned with GDPR**: Obligation in the settlement broadly aligned with similar GDPR obligations.
- **Implied by GDPR**: Obligation in the settlement is not explicitly present in the GDPR but implied via one of its provisions or via the accountability principle.
- **Goes beyond GDPR**: Obligation is not explicitly or impliedly required by GDPR.

Leadership and Oversight	
Facebook Obligations	**GDPR**
Section VII(C): • Obligation to establish, implement and maintain a comprehensive privacy program. • Designate compliance officers, including a CPO for product.	**Implied by GDPR**: • Implied via the GDPR accountability principle under Article 24 requiring organizations to put in place policies, procedures and measures implementing the GDPR requirements and to be able to demonstrate such implementation. • Under Article 37 of the GDPR, there is a requirement to appoint a Data Protection Officer (DPO) but the Facebook Settlement is more specific and granular with respect to such appointment (e.g. must appoint a CPO for Product; must be appointed by the independent privacy committee).
Section X: • Obligation to set up an independent privacy committee with independent directors.	**Goes beyond GDPR**: • The GDPR does not require setting up an independent privacy committee.
Section XI: • CEO and designated compliance officer must annually certify to the FTC that the company has established, implemented and maintained a privacy program that complies with the privacy program requirements of the order (i.e. requirement of internal certification).	**Goes beyond GDPR**: • Certification is performed by external third parties on a voluntary basis. • The EDPB currently takes the view that GDPR certifications will cover specific processing operations rather than an organization's entire privacy management program.
Section VII(E)(2) and Section XI: • Obligation to implement reporting and internal certification requirements.	**Implied by GDPR**: • Reporting obligations and internal certification are implied under the GDPR (e.g. internal audits are referenced in respect of compliance monitoring tasks of DPOs under Article 39).

Risk Assessment	
Facebook Obligations	**GDPR**
Section VII(D): • Assess and document at least once a year the internal and external risks in each area of the company's operation to the privacy, confidentiality or integrity of covered information (e.g. employee training; developer operations; partnerships with third parties; sharing of information; product research, design, development, marketing and implementation).	**Implied by GDPR**: • GDPR incorporates a risk-based approach to privacy, requiring organizations to assess the risks of harm to individuals and the benefits that are associated with the specific uses of personal information, thereby enabling risk mitigations that are tailored to the specific risk/benefit assessment. • Article 24 of the GDPR requires that the privacy program must be designed based on risk. • Although conducting risk assessments are impliedly required, the GDPR does not mandate yearly risk assessments.
Section VII(E)(2)(a)&(b): • Obligation to conduct a privacy risk assessment prior to new or modified product, service or practice implementation and to document such implementation in a "Privacy Review Statement".	**Aligned with GDPR**: • Article 35 of the GDPR requires data protection impact assessments to be carried out for high risk processing. • Data protection impact assessments must be documented under the GDPR in order to demonstrate accountability.
Section V: • Obligation to implement and maintain a comprehensive security program containing safeguards appropriate to the company's size and complexity, the nature and scope of its activities and the sensitivity of data.	**Aligned with GDPR**: • Article 32 of the GDPR requires implementing technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, costs of implementation, the nature, scope, context and purposes of processing.

Policies and Procedures	
Facebook Obligations	**GDPR**
Section VII: • Obligation to establish, implement and maintain a comprehensive privacy program.	**Implied by GDPR**: • Implied via the GDPR accountability principle under Article 24 requiring organizations to put in place policies, procedures and measures implementing the GDPR requirements and to be able to demonstrate such implementation.

Section II: • Obligation to implement procedures to obtain user affirmative express consent before sharing non-public user information with a third party where such sharing exceeds a user's privacy restriction settings.	**Aligned with GDPR**: • Sharing non-public user information with a third party in ways that exceed user privacy restriction settings would require opt-in consent under the GDPR, unless another legal ground applies (e.g. legitimate interest, contractual necessity or compliance with a legal obligation).
Section III: • Obligation to implement procedures on deletion of data (i.e. access by third parties and deletion from company servers) after user has deleted the information or terminated the user account and to delete the data within specified timeframes contained in the order.	**Implied by GDPR**: • Implied via Article 5 storage limitation principle and Article 17 right to erasure. • GDPR does not impose specific time thresholds for deletion though it imposes some general time limits (e.g. erasure of data without undue delay).
Section IV: • Obligation to implement procedures to limit the use or sharing of telephone numbers specifically provided to enable account security features.	**Implied by GDPR**: • Implied via Article 5 purpose limitation principle.
Section V: • Obligation to implement and maintain a comprehensive security program.	**Implied by GDPR**: • Article 32 of the GDPR on security of processing requires implementing technical and organizational measures to ensure a level of security appropriate to the risk.
Section VI: • Obligation to implement procedures relating to facial recognition technology (i.e. for certain users, not create any new facial recognition templates and delete existing templates unless the company discloses how it will use and share the templates to users and obtains their explicit consent).	**Implied by GDPR**: • GDPR does not explicitly address obtaining consent for using/sharing facial recognition templates but such a requirement is implied by Article 9 requiring explicit consent to process biometric data (note that this requirement may also go beyond GDPR where other Article 9 processing grounds are applicable).
Section VII(D): • Obligation to assess and document security breaches.	**Aligned with GDPR**: • Article 33 rules on data breach notification and Article 30 requirements to maintain records of processing.
Section VII(E)(1)(a)&(b): • Obligation to obtain self-certification from covered third parties that obtain or have access to personal information held by the company on an annual basis. "Covered Third Party" means any entity that receives information from the company other than a service provider acting under the direction of the company. The company must terminate access for failure to certify unless third party cures within 30 days.	**Goes beyond GDPR**: • While Article 28 requires controllers to carry out processor due diligence, there is no explicit mandate to carry out due diligence on data sharing partners, though such a requirement is implied via the accountability principle. • The GDPR does not mandate how third party due diligence must be carried out (i.e. third party self-certification is not mandatory).

Section VII(E)(3): • Obligation to design, implement and maintain access policies and controls for employees.	**Implied by GDPR**: • Implied via Article 5 integrity and confidentiality principle and Article 32 security obligations.
Section VII(E)(4): • Obligation to implement and maintain policies and safeguards for the sharing of personal information with company affiliates.	**Implied by GDPR**: • Implied via Article 5 integrity and confidentiality principle and Article 32 security obligations.
Section VII(H): • Obligation to select and retain service providers that can safeguard the covered information they receive from the company and contractually require them to do so.	**Aligned with GDPR**: • Aligned with Article 28 rules concerning the obligations of data processors.
Section XIV: • Obligation to create certain privacy related records for 20 years and to retain each such record for 5 years.	**Goes beyond GDPR**: • While Article 30 of the GDPR requires organizations to maintain records of processing activities, in line with the obligation to demonstrate accountability under Article 24, the Facebook Settlement is more prescriptive and imposes specific record retention periods.

Transparency	
Facebook Obligations	**GDPR**
Section I: • Prohibition against misrepresentation on the extent to which the company maintains the privacy and security of covered information.	**Aligned with GDPR**: • Aligned with Article 5 principles on lawfulness, fairness and transparency and purpose limitation. • Aligned with Articles 13 and 14 outlining transparency requirements.
Section II: • Obligation to disclose information to the user about the sharing of non-public user information with third parties that exceed a user's privacy restriction settings (i.e. categories of data that will be shared, identity of third parties and the fact that such sharing exceeds the privacy restriction settings imposed by the user).	**Aligned with GDPR**: • Aligned with Article 5 principles on lawfulness, fairness and transparency and purpose limitation. • Aligned with Articles 13 and 14 outlining transparency requirements.
Section VI and Section VII(E)(5): • Obligation to clearly and conspicuously disclose to users how the company will use and share facial recognition templates for users.	**Aligned with GDPR**: • Aligned with Articles 13 and 14 outlining transparency obligations and requiring notice for each specific processing operation.

Training and Awareness	
Facebook Obligations	**GDPR**
Section VII(G): • Obligation to establish regular privacy training programs for all employees on at least an annual basis.	**Implied by GDPR**: • Implied via Article 39 tasks of the DPO which requires informing and advising employees who carry out processing of their obligations under the GDPR and via Article 47 Binding Corporate Rules (BCR) which requires that BCR specify the appropriate data protection training to personnel having permanent or regular access to personal data.

Monitoring and Verification	
Facebook Obligations	**GDPR**
Section VII(D) and (F): • Obligation to assess and document at least once a year the internal and external risks in each area of the company's operation. • Obligation to assess, monitor and test at least once a year and promptly following the resolution of a covered incident, the effectiveness of any safeguards put in place to address the risks and modify the privacy program based on the results.	**Implied by GDPR**: • Implied via the risk-based approach incorporated in the GDPR, the accountability requirement of Article 24 and the requirement in Article 33 to document any personal data breaches and the remedial action taken (note that covered incidents are defined more broadly under the Facebook Settlement).
Section VII(E)(2) and Section XI: • Obligation to implement reporting and internal certification obligations (e.g. obligation to conduct a privacy risk assessment prior to new product implementation and document it in a "Privacy Review Statement"; obligation to deliver from the designated compliance officer to the CEO and Assessor a quarterly report containing a summary of the Privacy Review Statements and how the risks were identified and addressed; obligation to deliver a copy of the quarterly report to the FTC, upon request; obligation to certify to the FTC on an annual basis that the company has established, implemented and maintained a privacy program that complies with the privacy program requirements of the order. The certification must be signed by the CEO and designated compliance officer).	**Goes beyond GDPR**: • Reporting obligations and internal certification are implied under the GDPR but not to the extent of some of the measures required by the FTC in the Facebook Settlement (e.g. quarterly reporting to a data protection authority on request is not required under the GDPR).

Section VII(E)(1)(c): • Obligation to monitor third party compliance with the company's platform terms through measures including, but not limited to, ongoing manual reviews, automated scans, regular assessments, audits or other technical and operational testing at least once a year.	**Goes beyond GDPR**: • While Article 28 requires controllers to put in place contracts with processors and as a result monitor processor compliance with contractual obligations, the GDPR does not require such contracts to be put in place with data sharing partners, though in practice every company will most likely put such contracts in place.
Section VII(I): • Obligation to consult with and seek guidance from, independent, third party experts on data protection and privacy in the course of establishing, implementing, maintaining and updating the privacy program.	**Goes beyond GDPR**: • The GDPR does not require organizations to consult independent third party experts with respect to building and maintaining the privacy program.
Section VII(J): • Obligation to evaluate and adjust the privacy program in light of any material changes to the company's operations or business arrangements, a covered incident, new or more effective technological or operational methods to control identified risks and any other circumstances that may have a material impact on the effectiveness of the privacy program.	**Aligned with GDPR**: • Aligned with Article 24(1) which requires measures to ensure compliance with the GDPR be reviewed and updated where necessary and with Article 39 tasks of the DPO which requires monitoring compliance with the GDPR.
Section VIII: • Obligation to obtain initial and biennial assessments of the privacy program from one or more qualified third party professionals for a period of 20 years after issuance of the order.	**Goes beyond GDPR**: • The GDPR does not contain a requirement to obtain biennial assessments of privacy programs for set periods of time. This measure has been a unique feature of FTC consent decrees for many years.

Response and Enforcement	
Facebook Obligations	**GDPR**
Section VII(E)(1)(d): • Obligation to implement safeguards to enforce against any third party violations of the company's platform terms based on specific limiting factors.	**Goes beyond GDPR**: • The GDPR does not mandate enforcing against violations of company platform terms by independent third parties. The focus is on enforcing contractual terms to be upheld by processors.
Section IX: • Obligation to report covered incidents to the assessor and the FTC.	**Aligned with GDPR**: • Aligned with Article 33 and 34 breach reporting obligations. Note, however, the GDPR may require notification to the data subject, while the Facebook Settlement requires notification to the assessor.

IV. Equifax Settlement Requirements Mapped to the Elements of Organizational Accountability

The recent Equifax Settlement, related to its 2017 data breach, imposes a similar structure of requirements to that of the Facebook Settlement.[12] For instance, the Equifax Settlement requires the company to establish, implement and maintain a comprehensive information security program which involves measures such as:

- Designating a qualified employee or employees to coordinate, oversee and be responsible for the program and providing the written program and evaluations and updates to the Board of Directors or other equivalent governing body or senior officers (i.e. Leadership and Oversight);

- Assessing, at least once a year, the internal and external risks to the security, confidentiality and integrity of personal information and designing, implementing, maintaining and documenting safeguards that control for the material internal and external risks (i.e. Risk Assessment);

- Adopting policies and procedures to implement and monitor the information security program (e.g. patch management, remediation of high-risk security vulnerabilities, IT network and assets protection, data access controls, encryption and tokenization, vendor management etc.) (i.e. Policies and Procedures);

- Accurately outlining the extent to which the company maintains and protects the privacy, security, confidentiality or integrity of any personal information (in other words, the company is prohibited from making any misrepresentations in this regard) (i.e. Transparency);

- Establishing regular information security training programs, including at a minimum at least annual information security training for all employees and training for software developers relating to secure software development principles (i.e. Training and Awareness);

- Assessing, at least once every twelve months, the sufficiency of any safeguards in place to address the risks to personal information, and evaluating and implementing any needed modifications to the information security program based on the results. Additionally, the company must evaluate and adjust the information security program in light of any changes to the company's operations or business arrangements (i.e. Monitoring and Verification); and

- Establishing a clear and easily accessible process overseen by a senior corporate manager for employees to submit complaints or concerns about the company's information security practices, including establishing a clear process for reviewing, addressing, and escalating employee complaints or concerns. Additionally, the company must report security incidents to the FTC within a reasonable time after the date of discovery (i.e. Response and Enforcement).

- Annually provide the written information security program, material evaluations and updates to the Board of Directors, other equivalent governing body or senior officers
- Designate qualified employee(s) to coordinate, oversee and be responsible for the information security program
- Company must certify annually to the FTC that information security program has been established, implemented and maintained in line with order. Certification must come from the Board of Directors, other equivalent governing body or senior officers

- Process for receiving/addressing security vulnerability reports from 3rd parties
- Process for employees to submit complaints or concerns about the company's information security practices and procedures for responding to these
- Report security incidents to the FTC

- Annually assess the safeguards put in place to address the risks to security and modify program based on results
- Evaluate and adjust the program in light of any changes to the company's operations/business arrangements
- Vulnerability testing of company network
- Annual penetration testing of company network
- Obtain initial and biennial assessments of the security program from a qualified 3rd party professional (i.e. Assessor)
- Deliver quarterly report summarizing all breaches to Board of Directors, other equivalent governing body or senior officers

- Assess and document at least annually the internal and external risks to the security of personal information
- Design, implement, maintain and document safeguards that control for the material internal and external risks
- Assess the security of externally developed applications used within the company's technology environment

- Annual information security awareness training for all employees
- Training for software developers relating to secure software development principles

- Prohibition against misrepresentation of extent to which company maintains privacy/security

- Establish, implement and maintain a comprehensive information security program

Establish policies and procedures for:

- Patch management
- Assessing and documenting breaches
- Remediating high-risk security vulnerabilities
- Documenting a comprehensive IT asset inventory
- Protecting against network/host intrusion
- File integrity monitoring
- Limiting unauthorized network/system access
- Vendor management
- Data access control
- Encryption/tokenization
- Maintenance of records
- Ensuring use of secure development practices for applications developed in-house

Figure 2 – Equifax Settlement Requirements Mapped to CIPL "Accountability Wheel"

* Note: Some of these controls may be relevant to more than one accountability element.

V. Practical Implications of the Recent FTC Settlements

It appears from the above analysis that the requirements of the Facebook and Equifax settlements are in line with the essential elements of accountability and also potentially increase, in meaningful ways, the baseline expectations for any organization's accountability program. It is important to note, however, that while both settlements appear to redefine and provide greater insight into the FTC's expectations around corporate accountability programs for privacy and security compliance and raise the bar for the measures expected of large organizations, for example in terms of considering appropriate third party oversight, the specific terms of the orders are unique to the organizations subject to them and do not necessarily set the standard in terms of specific compliance measures that would be expected from all companies. Rather, the settlements reaffirm that the FTC expects all organizations to have "structurally" similar programs in that they must cover all core elements of accountability and will look for this structure in an investigation. Of course, companies must develop the specifics of their program based on the involved context (e.g. size and nature of the business, types and extent of data processing involved, existing and complementary controls for addressing multiple risks, etc.).

Moreover, it is important to remember that these settlements comprise contractual agreements with the FTC. They are not mandated orders in the sense that the final agreements involved negotiation and agreement by the parties involved. Therefore, the focus by companies, in looking at the settlements, should not be on the granular requirements but on the bigger picture of what elements comprise an accountable privacy and data security compliance program in the eyes of the FTC.

<u>Company Checklist – Elements of Privacy Management Programs</u>

The following is a checklist of best practices that companies can draw from both settlements, as they design and implement their privacy management programs.

Leadership and Oversight

- ☐ Designate appropriate personnel responsible for privacy and security compliance
- ☐ Ensure governance and accountability at the operation level, board and senior management level as well as appropriate reporting channels between operational staff and senior executives.
- ☐ Demonstrate the privacy program's establishment and effectiveness, internally to members of the organization and externally to business partners and data protection authorities on request.

Risk Assessment

- ☐ Assess and document the risk to individuals of all processing operations and where necessary, carry out privacy impact assessments.
- ☐ Continually review the program and update it in light of any novel risks posed by new or modified products, services, business practices or other processing operations.
- ☐ Design and implement controls to address not only privacy risks but also risks to the security of personal information.

Policies and Procedures

- ☐ Design and implement appropriate written policies and procedures to operationalize legal requirements and comply with applicable regulations, industry standards, regulatory orders (i.e. consent decrees or enforcement decisions from data protection authorities), as well as the values and goals of the organization.

- ☐ Implement relevant information sharing policies (e.g. with third parties and company affiliates), security policies and breach response procedures, data retention and deletion policies, policies for specific technologies (e.g. facial recognition), vendor management policies and due diligence procedures, employee data policies (e.g. HR rules, access control procedures), records management policies, etc.

Transparency

- ☐ Provide customers and business partners with appropriate and accurate notice about data practices, policies and procedures and how the company protects privacy and security.

- ☐ Provide appropriate information about data uses and the purposes and risks of processing and update customers and business partners where the purposes or the risks change.

Training and Awareness

- ☐ Conduct regular training programs for employees to ensure that they are aware of the privacy and security program and understand what action is required as part of their role to ensure compliance with the program.

Monitoring and Verification

- ☐ Assess, monitor and test the implementation and effectiveness of the privacy program on a regular basis.

- ☐ Consider, in addition to procedural controls, technical controls for ensuring that the organization's policies and procedures and other privacy restrictions are respected.

- ☐ Depending on the results of any auditing and testing process or in light of any material changes to business processes, practices or technology utilized, update the privacy program to address any new risks.

- ☐ Proactively monitor third party compliance with contractual restrictions and terms as well as policies on accessing and using data under the company's control (e.g. in the case of service providers who will be contractually bound to adhere to such policies).

Response and Enforcement

- ☐ Have procedures in place to address and report data incidents.

- ☐ Implement procedures for handling consumer complaints and have a clear process in place for reviewing and addressing such complaints.

- ☐ Implement procedures to enforce against non-compliance internally and from third-parties that use and access data under the control of the organization.

Scalability and Relevance of the Recent FTC Settlements for All Organizations

Although both the Facebook and Equifax settlements involve very large corporations, organizational accountability is a scalable concept and the general measures outlined above can be equally implemented by SMEs and startups in a manner that is proportionate to the risks within their specific business contexts. To better facilitate the implementation of accountability in line with the recent FTC consent decrees, CIPL believes there is a need to develop formal accountability schemes which can particularly assist smaller companies with implementing the relevant requirements to achieve and demonstrate accountability. Examples of such schemes include certifications, privacy codes of conduct (such as the APEC CBPR) and ISO standards. The same approach should be followed by the public sector and government agencies.

In addition, it follows from the recent FTC settlements that third party oversight and monitoring is integral to ensuring and demonstrating accountability. This includes traditionally required oversight of data processors but may also require organizations to consider oversight of independent third party data sharing partners, where appropriate and necessary. Furthermore, organizations that are not consumer-facing but only operational in B2B contexts will equally be required to have accountable privacy management programs in place to ensure the responsible use and handling of personal data.

Finally, it is important to note that by implementing a corporate privacy compliance program based on the essential elements of accountability, organizations in all industries, regardless of their size and type of business, are setting themselves up for global compliance with privacy and security laws no matter where they are located, including the GDPR, US state privacy laws and security rules,[13] Canadian data privacy law,[14] privacy regulations in Latin America,[15] Asia[16] and elsewhere.

Conclusion

While organizational accountability has been a hallmark requirement of FTC consent decrees for many years, recent FTC settlements have indicated that the FTC's vision of what constitutes an accountable privacy and security management program is evolving. This evolution is in line with accountability's global meaning in data protection and reflects a new compliance expectation for organizations whose data practices have equally evolved to keep pace with the data economy. By implementing a privacy and security compliance program that integrates and maps to each of the essential elements of accountability, organizations can ensure that they are taking appropriate measures to comply with modern data protection law and practice, are fulfilling the expectations of the FTC and other privacy enforcement authorities around the globe and, most importantly, are handling and protecting data in a way that is responsible and best fit for the modern digital age.

If you have any questions about this paper or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Sam Grogan, sgrogan@huntonAK.com; Matthew Starr, mstarr@huntonAK.com or Giovanna Carloni, gcarloni@huntonAK.com.

References

[1] See CIPL White Paper on "The Concept of 'Organizational Accountability' - Existence in US Regulatory Compliance and its Relevance for a Federal Data Privacy Law", 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_-_existence_in_us_regulatory_compliance_and_its_relevance_for_a_federal_data_privacy_law__3_july_2019_.pdf.

[2] See for example, In the Matter of Google Inc., Docket No. C-4336, 13 October 2011, available at https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf and In the Matter of Facebook Inc., Docket No. C-4365, 27 July 2012, available at https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[3] For example, In the Matter of Snapchat Inc., Docket No. C-4501, 23 December 2014, available at https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf. This consent order, while inclusive of many elements of accountability, contains just 6 pages of requirements. The recent Facebook and Equifax settlements (see notes 4 and 5 below) contain over 20 pages of requirements.

[4] United States of America v Facebook, Inc. – Stipulated order for civil penalty, monetary judgment and injunctive relief, Case No. 19-cv-2184, 24 July 2019, available at https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

[5] FTC v Equifax, Inc. – Stipulated order for permanent injunction and monetary judgment, Case No. 1:19-cv-03297-TWT, 23 July 2019, available at https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[7] (a) Office of the Privacy Commissioner for Personal Data, Hong Kong, Privacy Management Programme: A Best Practice Guide, August 2018 (revised edition), available at https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf; (b) the Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia, Getting Accountability Right with a Privacy Management Program, 2012, available at https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf; (c) Personal Data Protection Commission of Singapore, Guide to developing a data protection management programme, 2017 (revised July 2019), available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Guide-to-Developing-a-Data-Protection-Management-Programme-15-July-2019.pdf; (d) Office of the Australian Information Commissioner, Privacy management framework: enabling compliance and encouraging good practice, available at https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework; (e) National Institute for Transparency, Access to Information and Personal Data Protection, Principios rectores de la Protección de Datos Personales, available at http://inicio.inai.org.mx/GuiasTitulares/Guia%20Titulares-02_PDF.pdf; and (f) Superintendente Delegado para la Protección de Datos Personales, Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability), available at http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada.

[8] GPEN Sweep 2018 'Privacy Accountability', Office of the Privacy Commissioner, New Zealand and Information Commissioner's Office, UK, October 2018, available at https://ico.org.uk/media/about-the-ico/documents/2614435/gpen-sweep-2018-international-report.pdf. While the Federal Trade Commission is a member of GPEN, it was not able to participate in this particular sweep because it involved a "survey" style approach that was not in line with relevant rules on how the FTC may request information from companies.

[9] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 92 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern

information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[10] For a full discussion of organizational accountability in data protection, see CIPL white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; and CIPL Accountability Q&A, 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf.

[11] Please note that Section XII (Order Acknowledgements) and Section XV (Compliance Monitoring) of the Facebook Settlement relate to requirements that do not fall within the essential elements of accountability. Section XII requires Facebook to acknowledge receipt of the order to the FTC and deliver copies of the order throughout the organization for five years after the date of entry of the order and to obtain signed acknowledgement of receipt of the order from each individual or entity to whom it is delivered. Section XV requires Facebook to assist the FTC with its own monitoring of Facebook's compliance with the order by submitting additional compliance reports or other requested information to the FTC within 14 days of receipt of the request and to permit the FTC to interview any employee or other company affiliates on matters concerning the order. This represents external monitoring of the privacy compliance program by the FTC rather than internal monitoring and verification as detailed in this paper.

[12] *Supra* note 5.

[13] The essential elements of accountability can be found in many US state privacy laws and security rules, including the NY Department of Financial Services Cybersecurity Regulations (23 NYCRR 500), the NAIC Insurance Data Security Model Law, the 2018 Vermont Data Broker Law (H.764) and the Massachusetts Standards for the Protection of Personal Information (201 CMR 17.00), among others.

[14] For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) (S.C. 2000, c. 5).

[15] For example, the Brazilian LGPD (Lei Geral de Proteção de Dados Pessoais).

[16] For example, the Philippines Data Privacy Act of 2012 and the Dubai International Financial Centre's proposed new data protection law.