BCLP. Client Intelligent

Insights

NAVIGATING THE FEMTECH REGULATORY LANDSCAPE

WHICH RULES APPLY AND WHAT ARE THE ENFORCEMENT PRIORITIES?
DIGITAL SPEAKS SERIES

May 16, 2024

SUMMARY

Security, scale or functionality – pick two. This computer science principle coined by the late Professor Anderson is particularly relevant to the FemTech industry. Anderson's Rule states that for a system to provide high functionality and security, its access may need to be limited (small scale); alternatively, offering high functionality on a larger scale, may require an acceptance of risk, e.g. of inadvertent or deliberate disclosure of information. In real life systems - including FemTech - a balance must be struck.

It is no surprise, then, that the regulatory landscape for FemTech is complex and fragmented. Different jurisdictions approach the question of health/medical data in diverse ways and apply different laws and standards to the protection of personal data. All these rules are ultimately intended to mitigate the risks to personal data posed by large databases of sensitive personal information while facilitating the benefits. In part two of our series, we examine the UK, EU and US regulatory privacy landscapes and enforcement priorities and how they apply to the FemTech sector.

For more, read our previous article "What is femtech and how can it meet the privacy needs of its users?".

LEGAL FRAMEWORK: EU & UK

In the EU and the UK, the General Data Protection Regulation (**GDPR**), and the UK GDPR and Data Protection Act 2018 (**DPA**) (respectively) provide a comprehensive framework for the processing of personal data, including special category data, such as health and biometric data. The GDPR and the DPA require controllers and processors to comply with principles such as lawfulness, fairness, transparency, data minimisation, security, and accountability, and to obtain valid consent or rely on another lawful basis for processing personal data. The GDPR and the DPA also grant individuals

rights to access, delete, rectify, restrict, or object to the processing of their personal data, and to lodge complaints with the relevant supervisory authorities.

Additional e-privacy regulations (Directive 2002/58 and the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003) apply to the use of "cookies" and similar technologies online, as well as requiring prior consent to collect location data and to send electronic marketing.

The focus of this piece is on the data protection rules, but they are only one part of the UK's regulatory mosaic. For example, in the UK, advertisers in the FemTech space must comply with the ASA's non-statutory CAP Code when making claims in a fertility app. In recent years, the ASA has upheld complaints about misleading claims made in relation to products claiming to reduce or eliminate menopause symptoms, as well as providing recent guidance about how private clinics can market pregnancy ultrasound services within CAP guidelines. In June 2021, the ASA, jointly with the Medicines and Healthcare Products Regulatory Agency (**MHRA**) and the Competition and Markets Authority, also issued an enforcement notice to the fertility industry. This sets out how fertility clinics should advertise their prices, success rates, add-on treatments and complementary therapies, to comply with the CAP Code. FemTech developers also need to comply with medical devices regulations, with the MHRA overseeing implementation and enforcement of these regulations in the UK (medicinal claims can only be made for medicinal products/medical devices licensed by the MHRA). Overarching UK consumer law will also apply – which will have an impact on the content and presentation of online terms and conditions (particularly how pricing information is presented and understood by the consumer). New UK consumer rules are currently being considered by the UK Parliament and will also affect how products are offered on a subscription basis. These new rules specify the information to be provided to a consumer pre-contract, mandate the provision of reminder notices and require traders to provide user-friendly means for consumers to end or cancel a subscription contract, as well as the provision of cooling off periods.

LEGAL FRAMEWORK: US

Data protection in the US is not nearly as tightly and collectively regulated on a national level as the EU and UK. Much of the rulemaking has been left to the individual states to decide. On a federal level, The Privacy Act of 1974 (**The Privacy Act**) regulates how federal government agencies can collect, use and store an individual's personal data in their record systems. The Privacy Act also prevents the federal government from disclosing certain personal information they have collected without the written consent of the individual. The Privacy Act is subject to some limited exceptions mostly associated with the US Census Bureau's use of statistical information that is not individually identifiable, but the Privacy Act, along with most other federal privacy laws (The Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy

Act, the Video Privacy Protection Act, etc.) allow the individual states to craft protections that go further than the baselines established by the federal government.

One federal law that goes a bit further on regulating personal health information is The Health Insurance Portability and Accountability Act (**HIPAA**). HIPAA was signed into law by President Bill Clinton in 1996 and regulates how physicians and other medical and healthcare providers, as well as covered entities (e.g., healthcare insurance companies, healthcare clearinghouses and others) can collect, use and store a patient's personal health data. Many Americans erroneously believe that HIPAA has a much broader reach as it concerns health-related information, but it only covers personal health information created in a clinical setting or context. Any information that was not created or shared in a clinical setting or context, for example information shared on a weight loss or nutrition app, or stored on an electronic device like a smart watch, would not be protected under HIPAA. It is worth staying on top of this regime in particular as discussions from researchers and advocacy groups have steadily increased calling for the expansion of HIPAA regulations and for the federal government to fill the gap to safeguard individual health data on personal technology devices in particular.

Instead of an all-inclusive federal law focused on data protection similar to the GDPR or the DPA, individual states have enacted their own laws to tightly regulate how companies can use consumer data. This means FemTech developers must be vigilant in understanding how their products and practices are regulated, not only nationally, but also on a state-by-state basis.

The following states have passed heightened privacy legislation, more restrictive than federal standards: California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah and Virginia, with at least ten other states introducing similar legislation. While each state's legislation differs from the other, they all have the common trend of protecting individuals' data. Since California was the first state to adopt such legislation, many states will follow its requirements. The California legislation, called the California Consumer Privacy Act (**CCPA**), as amended by the California Privacy Rights Act (**CPRA**), adopted three GDPR principles: (i) data minimization, (ii) storage limitation and (iii) purpose limitation. These GDPR-mirrored principles restrict or limit a company's retention and collection practices of personal data. Also similar to the GDPR is California's creation of the governing body, the California Privacy Protection Agency (**CPPA**). The CPPA applies to for-profit businesses that conduct business in California and meet any of the following three criteria: (i) have a gross revenue of over $25 million, (ii) buy, sell, receive or share personal data and information of 100,000 or more California residents or households, or (iii) collect 50 percent or more of its annual revenue from selling the personal information of California residents. Any FemTech company that falls into those categories will be compliant with California's requirements if it follows these steps: (i) deliver an "at time of collection" privacy policy to consumers that explains all of their rights as the consumer, (ii) honor any consumer requests for retraction, deletion or sharing of personal information, (iii) allow

consumers to submit requests for handling their personal information, and (iv) adopt safety features to protect consumers' personal information.

Even though the US is behind compared to the EU and the UK, federal privacy laws are on the horizon. On April 7, 2024, congressional leaders presented a discussion draft of the American Privacy Rights Act (**APRA**), a federal comprehensive consumer privacy bill. The APRA does not apply to small businesses (those with $40 million or less in revenue, collect information of 200,000 or less individuals, and do not earn revenue from selling data to third parties). If passed, the APRA would require companies to allow consumers to opt-out of targeted advertising, ask companies to completely delete their data, receive data in a portable format and other practices. Other similar legislation has been introduced before, but since many states adopted their own laws, the issue of preemption stops the federal law from passing.

ONLINE ADVERTISING UNDER SCRUTINY

The UK and the EU regulators are currently scrutinising the online advertising sector, especially the use of tracking technologies, such as cookies, and the practice of real-time bidding, which involves the auctioning of personal data to advertisers in milliseconds. We are seeing particular concerns in the EU about certain models of targeted advertising, with the European Data Protection Board taking an increased interest in tracking and behavioural advertising and being asked to give a view on the so-called 'pay or ok' targeted advertising model (where you either pay for your account and receive it on an ad-free basis or choose to accept targeted advertising as part of the terms on which you use the product for free).

US regulators are also focusing on governing online advertising practices. The Federal Trade Commission (**FTC**) released Behavioral Advertising Principles that outline how websites should treat visitors. The FTC advises that websites should allow visitors to opt-out of data collection, such as cookies.

UK REGULATORY STANCE AND ENFORCEMENT ACTIVITY

In the UK, prior to September 2023, the regulator responsible for enforcing and promoting data protection compliance – the ICO - had not focused directly on the FemTech industry. The closest enforcement activity involved fining a parenting advice site for selling the personal data of a large group of new mothers and fining a parenting club for sharing personal data with data brokers and credit reference agencies.

Since that time, the ICO has:

- launched a review of period and fertility tracking apps (in September 2023). This concluded in February 2024, with the ICO deciding that while no serious compliance issues or evidence of

harms were identified in its review, all app developers should be alive to the importance of protecting users' personal information, especially where sensitive information is involved;

- also issued an enforcement warning in November 2023 to websites that use cookies for advertising purposes, requiring them to provide clear and granular choices to users, and to avoid 'nudging' of users or the bundling of consent to advertising with the terms of use. It also wants the cookie opt-out to be easy for users to operate. As part of this, the ICO has specifically indicated that women being targeted by online adverts (for example, seeing baby adverts shortly after miscarriage) forms part of the rationale for this enforcement activity; and

- issued guidance to improve transparency in health and social care, to provide regulatory certainty for health and social care organisations as to how they ensure they are transparent with individuals about how their personal data will be used.

The ICO has also published new guidance on how it exercises its powers to issue penalty notices and fines. Factors impacting the level of fine include the nature, gravity and duration of the compliance failure. For example, 'high risk' processing may include processing operations that involve the application of new or innovative technology, automated decision making, the use of biometric or genetic data, monitoring or tracking or invisible processing. More weight may be given to these factors where there is a clear imbalance of power between the data subjects and the controller, the processing involves children's personal data or the processing involves personal data of other vulnerable people who need extra support to protect themselves. The ICO is therefore likely to consider infringements involving the processing of special category data as being particularly serious. This suggests that FemTech apps may soon be encountering more regulation with enforcement actions too.

EU ENFORCEMENT ACTIVITY

In the EU, we have not yet seen concerted enforcement action being taken at the *EU* level in relation to the FemTech sector. However, the Norwegian Consumer Council reviewed two period tracking apps and expressed concerns about the privacy settings and use of location data for advertising purposes. It also criticised the bundling of consent to data sharing with the overall consent to use the app, noting that this practice may affect the quality of the consent given by the user (and therefore the ability of the app to rely on that consent).

US ENFORCEMENT ACTIVITY

Both national EU member state regulators and the FTC in the US are also clamping down more generally on the misuse of users' location data, with the FTC recently banning data brokers from selling location . The FTC is increasingly focused on data protection, stating in 2022 that it will "vigorously enforce the law if [it] uncovers illegal conduct that exploits Americans' location, health, or other sensitive data." In 2024 alone, the FTC has taken action against at least thirteen

companies. As mentioned, many states are creating data protection laws and regulating bodies to enforce any noncompliance. California's governing body, the CPPA strictly enforces compliance with the state's privacy law. Since 2020, the CPPA has brought multiple actions against large health-related US companies. Most of the actions focused on each company's failure to receive consumer consent before selling their personal information and mishandling health information.

ON THE HORIZON IN 2024

Potential risks for those who do not comply with data protection legislation could include the threat of class actions, which might follow a negative regulatory finding, particularly in North America (such actions are not available as of right in the UK, unless a group action can be framed in competition law terms and brought in the Competition Appeals Tribunal). We see this being an increasing trend, particularly in the US, in the year to come.

The final article in our series sets out some best practice guidance addressing personal data issues for those in the FemTech industry.

RELATED CAPABILITIES

- Healthcare & Life Sciences

MEET THE TEAM

Seth C. Pearson

Atlanta

seth.pearson@bclplaw.com
+1 404 572 6614

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and

should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2025 Bryan Cave Leighton Paisner LLP.