SQUIRE PATTON BOGGS

FCC BECOMES LATEST AGENCY TO INCREASE CONSUMER PRIVACY AND DATA SECURITY ENFORCEMENT

As attention and related widespread concerns about data security and exposure of sensitive private consumer information grows around the US, the Federal Communications Commission (FCC) has joined the array of federal agencies using their enforcement tools to address these issues. While the Communications Act (Act) for many years has afforded confidentiality protections for the details of a consumer's phone bill, over the last year, the FCC – led in particular by its Enforcement Bureau – has demonstrated an increased willingness to more broadly and aggressively protect "the sensitive personal information of American consumers from misappropriation, breach, and unlawful disclosure." This trend continued when the Bureau issued an Enforcement Advisory on May 20, 2015, providing initial guidance regarding the protection of personal and proprietary information by retail broadband internet access providers (ISPs).

Traditional Privacy Focus

To be sure, under Section 222 of the Act, the FCC had always protected certain limited forms of customer information from misuse by those who collected it – primarily call detail information on individual phone bills (customer proprietary network information or CPNI). In 2013, the agency made clear that these protections applied equally to mobile carriers who collect such information. And most recently, last September, the agency settled a matter with Verizon for US$7.4 million involving the company's failure to notify its customers about Verizon using their CPNI for marketing. A series of more recent enforcement actions, however, reflect that the agency has expanded its focus well beyond traditional concerns about protecting CPNI.

Flexing Enforcement Authority

The opening salvo in this expanded campaign occurred last October when the FCC proposed fines of US$10 million on two telecommunications carriers that left unprotected, on publicly accessible websites, "proprietary information" they had gathered, including Social Security numbers. The FCC, in a 3-2 decision, concluded that Sections 222 and 201 of the Act impose a duty on carriers to protect such information, even though it was not the CPNI that the FCC had traditionally focused on in the past.

Then, in April of this year, the FCC entered into a US$25 million settlement with AT&T to address data breaches by company employees at call centers in Mexico, Columbia and the Philippines. Again, the enforcement action went beyond a focus on just CPNI to include the exposure of Social Security numbers and other identifying information.

To some degree these actions are not surprising. The Enforcement Bureau's senior leadership has substantial experience in data security and privacy protection, having worked in state attorneys general and other enforcement offices.

And Now the Internet: Enforcement Advisory

Without question the major expansion of the commitment to privacy protection is the application of Section 222 to ISPs as newly classified telecommunications carriers. While the FCC recognized that its existing rules focused on voice type services and CPNI protections were a mismatch, the agency announced a commitment to developing a privacy regime under Section 222 for ISPs. It started that process with a workshop in April, which did not tip the agency's hand as to how it would proceed with enforcement. But on May 20 the Bureau issued an Enforcement Advisory warning ISPs that, after the effective date of the Open Internet Order on June 12, 2015, the Bureau will focus on "whether broadband providers are taking reasonable, good-faith steps to comply with Section 222." The Advisory also noted that the Bureau expects such providers to "employ effective privacy protections in line with their privacy policies and core tenets of basic privacy protections."

There are several points worth noting. First, the Advisory explains that the Bureau is available to provide informal and formal guidance on "how best to comply with Section 222," and states that although requesting guidance in the form of an advisory opinion is not required, the existence of such a request will tend to show good faith. Second, the Bureau repeated that it will only advise on "anticipated" conduct, consistent with direction in the Open Internet Order that hypothetical situations or past/ongoing conduct will not be the subject of advisory opinions. Third, the Commission – and the Bureau acting on delegated authority – reserved the right to change course from previously issued advisory opinions. Finally, the FCC warned in the Order that it monitors press reports and other public information, which could lead to the initiation of an investigation.

Joining Forces

The FCC's focus on privacy protection is also reflected in its joining and publicizing its membership in international privacy groups. In April, the FCC joined the Asia Pacific Privacy Authorities, the principal international forum of privacy enforcement authorities in the Asia Pacific Region. This collaboration follows the FCC announcing its membership in the Global Privacy Enforcement Network, an international group of privacy enforcement regulators comprising approximately 50 data protection authorities. Significantly, in both of these memberships, it is the Enforcement Bureau that represents the FCC.

Going Forward

It is clear that the FCC has staked out a role for itself both domestically and internationally in the protection of sensitive personal information by an expanded group of companies that gather such information. The scope of the requirements – particularly as they relate to the Internet – remain evolutionary and jurisdictional issues will need to be sorted out. But there is no question that the FCC is committed in a significant way to being involved in issues surrounding the security of sensitive information. Squire Patton Boggs is well equipped both domestically and internationally to represent and advise clients as this regulatory evolution continues.

About Our Communications and Global Data Protection and Cybersecurity Practices

Spanning 44 offices in 21 countries, Squire Patton Boggs has substantial experience interacting with the FCC, other government agencies and Congress on consumer privacy, cybersecurity and data security issues. We have a comprehensive and integrated communications and cybersecurity team that has decades of experience navigating through these issues ranging from regulatory and compliance matters, investigations, internal audits and representation before the FCC. The team includes former FCC officials and enforcement staff, former senior Executive branch level officials, cybersecurity and privacy experts, including Certified Information Privacy Professionals (CIPP/US), as well as long-time practitioners before the FCC.

Contacts

Paul C. Besozzi
T +1 202 457 5292
E paul.besozzi@squirepb.com

Monica S. Desai
T +1 202 457 7535
E monica.desai@squirepb.com

Norma M. Krayem
T +1 202 457 5206
E norma.krayem@squirepb.com

Koyulyn K. Miller
T + 1 202 457 5321
E koyulyn.miller@squirepb.com