JOURNAL OF INTERNET LAW
VOLUME 18
NUMBER 2
AUGUST 2014
EDITED BY DLA PIPER

The NLRB's Continued Regulation of Social Media in the Workplace

By Sean J. Kirby and Eric Raphan

Virtually every major employer in the United States uses social media for business or promotional purposes, and millions of employees will take to Facebook or Twitter this year to discuss their personal and professional lives. Due to the increasing popularity of social media Web sites, employers have had to implement policies to delineate how employees may use social media in connection with their employment. In fact, more than 80 percent of businesses now have formal social media policies governing employee use of social media at work—an increase of 20 percent since just last year.[1] Given that employee use of social media shows no sign of slowing, the questions of: (i) when employers may use employee social media posts to justify adverse employment actions; and (ii) how employers should construct and enforce their social media policies, are ones that most employers will be forced to answer.

However, employers are not alone in determining how to deal with the foregoing questions. In fact, over the past few years, the National Labor Relations Board (NLRB or the Board) has issued a number of decisions addressing both terminations relating to social media posts and the lawfulness of employer social media policies. As discussed herein, recent Board decisions (which some employers may feel are overbroad and/or too restrictive in some instances), do provide employers with the insight and guidance they need to make employment-related decisions based on social media use and to implement effective social media policies.

Continued on page 13

Sean J. Kirby *is an associate at Sheppard, Mullin, Richter & Hampton LLP in New York, NY, and practices in the firm's Labor & Employment group.* **Eric Raphan** *is a partner at Sheppard, Mullin, Richter & Hampton LLP in New York, NY, and practices in the firm's Labor & Employment group.* Gregory Re, *a summer law clerk at Sheppard, Mullin, Richter & Hampton LLP, assisted in the preparation of this article.*

Wolters Kluwer
Law & Business

Amendments to the Turkish Internet Broadcasts and Publication Law, and the Controversial Application of the New Provisions

By Uğur Aktekin and Bentley James Yaffe

The main legislation in Turkey applying to information broadcast and published online is the Law numbered 5651 on the Regulation of Broadcasts and Publications Made Online and Regarding the Countering of Crimes Committed via These Broadcasts and Publications (Internet Publication Law) which came into effect upon publication on May 23, 2007. The Internet Publication Law introduced procedures for applying blocking orders to Internet Web sites that included content that constituted criminal offenses and also defined the responsibilities of content, hosting, and service providers. The law also introduced a mechanism for real or legal persons claiming that their rights were being infringed by online content, which enabled the claimant to first apply to the content or hosting provider and if the initial request was not addressed subsequently make an application to the courts for the removal of the infringing content.

However the omnibus law titled the Law Regarding the Amendment of the Decree Law on the Structure and Duties of the Ministry of Family and Social Policy and Other Laws and Decree Law (Omnibus Law) that entered into force after being published in the Official Gazette of February 19, 2014, introduced amendments to the Internet Broadcast Law. These amendments have been the subject of criticism and debate, as multiple critics have argued that they impose inordinate levels of state control over the use of the Internet and enable streamlined mechanisms for state censorship of Internet-based content. While this criticism had been voiced from the initial drafting of the Omnibus Law, many of the issues raised were not addressed when the Omnibus Law was sent for approval. After the approval of the Omnibus Law, some of these areas were addressed with subsequent legislative measures that came into effect as of publication in the Official Gazette of March 1, 2014. However, these subsequent measures also were criticized as not implementing sufficient changes to address the wider criticism of the Omnibus Law.

AMENDMENTS BY THE OMNIBUS LAW

RESPONSIBILITIES OF CONTENT, HOSTING, AND ACCESS PROVIDERS

The Internet Broadcast Law provided the definitions of content providers, hosting providers, and access providers and had established their responsibilities.

As per Article 4 of the Internet Broadcast Law, content providers were defined as "real or legal persons that produced, changed or provided any information or data that was provided on the Internet to users", hosting providers were defined as "real or legal persons that provide or run systems hosting services

Uğur Aktekin *is a partner at Mehmet Gün & Partners specializing in Intellectual Property (IP) law, and co-chairs the IP and T-M-T practices of the firm.* **Bentley James Yaffe** *is a trainee attorney at law at Mehmet Gün & Partners.*

and content", and access providers were defined as "any real or legal person that provides users with access to the Internet."

While these definitions were not changed by the amendments of the Omnibus Law, the responsibilities of each category were extended. An obligation was introduced for the very widely defined category of content providers, that will mean content providers will be obligated to provide the Telecommunication and Communications Directorate (Directorate) with the information they request, in the form that they request it be presented in order to aid the Directorate in the execution of their statutory duties. The same obligation also has been introduced for hosting providers and access providers. As this amendment does not provide any clear guidelines as to what information may be requested by the Directorate, the inclusion of such a provision seemingly would cause an undue burden on any provider and creator of online content and provider of hosting or Internet access services.

New obligations also have been imposed on hosting providers, namely the obligation to remove all offending content that falls under the scope of Articles 8, 9, and 9A of the amended Internet Publication Law and the obligation to store the traffic data for the services they provide for a duration that will be determined with a later directive, but which will be between one and two years. Hosting providers also will be responsible for the integrity and confidentiality of this stored traffic data.

The obligation to store the traffic data has led to concerns for hosting providers, as increased infrastructural burdens will require increased investment. Additionally, concerns have been voiced as the reasoning for an increase in the duration of storage of such traffic data has not been clearly stated. The aforementioned subsequent legislative measures that came into effect on March 1, 2014, have provided a reduced scope for the definition of user traffic data and have made it necessary for a court order in the scope of an investigation or prosecution to be presented before the Directorate can request such traffic data from the hosting providers.

The amendments to the Internet Broadcast Law have imposed an obligation on access providers regarding blocking orders that have been issued. If such a blocking order is issued, access providers will be under the obligation to block all access to the content, including any and all alternative means of access. This obligation has been criticized due to the unfair burden placed on access providers. As, under the amended Internet Publication Law, access providers face administrative fines ranging from TRY10,000 to TRY50,000 if they are in violation of their obligations, placing the burden of preventing all means of alternative access can be regarded as a too broad and technically impossible task for any access provider to undertake.

Another amendment introduced by the Omnibus Law that imposes stricter controls on the aforementioned parties related to the notification process. The amendment allows the classification of any communication to the aforementioned parties—domestic or foreign—via the communication tools on their Web sites, or email, or other means of communication directed to their contact information located through their domain name or IP address as an official notification. However, this amendment regarding notifications contravenes the current requirement under Turkish Law that regulates notification made to parties. Allowing such online communication tools and emails to be classified as official notification made to parties would seemingly undermine the certainty of attempted notification and cause issues relating to a fair right of reply.

THE ESTABLISHMENT OF THE ASSOCIATION OF ACCESS PROVIDERS

One of the most controversial aspects introduced by the Omnibus Law is the addition to the Internet Broadcast Law that established an organization called "The Association of Access Providers" (Association). This Association will comprise all Internet service providers and access providers and membership will be compulsory, with companies that are not members being banned from operating within Turkey. The centre of the Association will be in Ankara, and the charter and any such subsequent changes to the charter must be presented to the approval of the Directorate. The main duty of the Association, as defined by the amended provisions of the Internet Broadcast Law, will be the implementation of blocking orders issued under Article 9 and 9A of the amended Internet Publication Law. The Association is tasked with the provision of any hardware or software required for such implementation.

The Association also will serve as the representative of all the parties engaged in Internet related services, with all notification or blocking orders notified by the Directorate to the Association accepted as having been made to the individual party/company that the notification or blocking order relates to. In their role as representative of the industry, the Association also will have standing to appeal against any notification or blocking order made by the Directorate.

The establishment of such an organization, that will have compulsory industry-wide membership and which is so closely connected to and supervised by the Directorate could be interpreted as extending state control over the private sector parties engaged in the provision of Internet related services. Additionally, the establishment of such an Association that requires compulsory membership with membership fees to be determined based proportionally on each member's net sales will increase operating costs for companies providing these Internet services.

BLOCKING ORDER APPLICATIONS

Under the previous version of the Internet Broadcast Law, blocking orders were provided under Articles 8 and 9.

Article 8 addresses the blocking of access to certain content that is illegal under the Turkish Criminal Code, and grants prosecutors and judges the right to issue blocking orders for situations in which content features one or more of the catalogue crimes listed in the Article. These catalogue crimes cover the following crimes as listed in the Turkish Criminal Code; the inducing of suicide, sexual abuse of children, facilitating the use of narcotics, procuring substances that are harmful to health, obscenity, prostitution, and the provision of a location and opportunity for gambling. Along with the catalogue crimes that fall under the scope of the Turkish Criminal Code, Article 8 also gives prosecutors and judges the right to issue blocking orders against content that insults the memory of Mustafa Kemal Atatürk, the founder of the Turkish Republic.

The Omnibus Law introduced two significant amendments to Article 8. The first amendment was that judicial authorities can now issue a blocking order that is limited to a set period of time and will expire after such a time has passed. The second and more significant amendment has replaced the sanction of a prison sentence for access providers or hosting providers that fail to comply with the blocking order with a sanction of a criminal fine.

The Omnibus completely redrafted Article 9 and introduced an additional article titled Article 9A.

Article 9 relates to cases where a legal or real person's personal rights have been violated. In such cases, under the provisions of the amended Article 9, the person may apply to the content provider, the hosting provider or apply directly to the criminal court of peace. The content provider or hosting provider is obligated to answer the applicant within 24 hours of being contacted, and similarly the criminal court of peace is obligated to evaluate the application within 24 hours.

If an application has been made to the court and if the court judges the application to be valid, a decision for a partial or full blocking of access can be issued and subsequently notified to the Association of Access Providers. The Association must then implement said blocking order within four hours of receipt. It is important to note that under the provisions of the amended Article 9, issuing a blocking order for an entire Web site is listed as an exception with the legal norm being stated as issuing a blocking order only for the sections containing the offending content. An example of this would be for the court to order a blocking order for specific URL's that have been identified as featuring the offending content. While this decision of the courts can be appealed, the blocking order will stand during such an appeals process.

Additionally, under the provisions of the article that was redrafted by the Omnibus Law, if the offending content that was the subject of the blocking order issued by the court is featured on another Web site or another section of the original Web site, the applicant may directly approach the Association for the blocking of such content without needing to seek a further court order.

Even though such a process for issuing a blocking application also existed under the previous Internet Broadcast Law, the applicant could only apply for a court issued blocking order if the applicant's notification to the content provider or hosting provider was not answered within two days. The previous form of Article 8 also included strict sanctions for cases of non-compliance with a court issued blocking order in

the form of a prison sentence ranging from six months to two years. With the amendments introduced by the Omnibus Law, the sanction of a possible prison sentence for those who fail to implement court issued blocking orders has been replaced with the sanction of a criminal fine.

Article 9A of the Internet Broadcasts Law as introduced by the Omnibus Law has implemented a completely different process of blocking order application. This process is based on the grounds of "violation of personal privacy" and it is limited to real persons only. In a situation where the right to personal privacy is violated by online content, real persons have been granted the right to apply directly to the Directorate for the issuing of a blocking order.

If the Directorate decides to issue a blocking order, the subsequent notification to the Association must be implemented within four hours. The applicant must then apply to the criminal court of peace within 24 hours in order to gain a court issued blocking order. If the court does not grant such an order within 48 hours of the application, the initial blocking order implemented by the Directorate automatically will be removed. The decision of the criminal court of peace can be appealed through the courts. Article 9A also grants the Directorate the authority to block access to the content itself without notification to the Association, if it is deemed that a delay in blocking the content will prove detrimental to the protection of personal privacy. As per the initial provisions introduced by the Omnibus Law, this blocking administered by the Directorate could be appealed by application to the criminal court of peace, with the Directorate not being required to seek prior judicial or administrative authorization before implementing such a blocking of content. However, with the introduction of the aforementioned new legislative measure that came into effect on March 1, 2014, in the situation that the Directorate issues such a blocking of content, they must submit this decision for approval to the criminal court of peace within 24 hours. The judge must then rule on the matter within 48 hours.

The second administrative route of issuing blocking orders by empowering an administrative body that lacks the accountability of the courts with the right to directly block access to content and Web sites can been criticized as undermining the certainty and accountability of legal processes. This is particularly emphasized in the examples of the blocking orders issued against Twitter and Youtube. In both of these cases the Directorate was accused of going beyond the scope of authority that has been granted to them by the Internet Broadcast Law.

THE BLOCKING OF TWITTER AND YOUTUBE

On March 20, 2014, citing the new provisions of the amended Internet Broadcast Law the Directorate implemented a protection order that blocked access to the micro-blogging Web site Twitter. The blocking of access to the Web site made it impossible to access any of the pages using browsers or mobile applications.

On the database of the Information and Communication Technologies Authority (Authority), the grounds for the blocking order against Twitter were listed as three court decisions, and another decision issued by the Istanbul Chief Prosecutor's Office. The Authority also issued a statement a day after the blocking order was implemented, stating that court decisions concerning the violation of personal rights and the rights to privacy had been notified to the Authority, that these decisions relating to the removal of content were then notified to Twitter, but as Twitter had not complied with these requests it was deemed necessary to block access to the entire Web site in accordance with the provisions of the Internet Broadcast Law. The Authority also stated that should Twitter remove said content and undertake to apply the rulings made by Turkish Courts, access to the Web site would be restored.

Matters also were complicated by the fact that under the provisions of the amended Internet Broadcasting Law, service providers were under the obligation to block all alternative technologies that could be used to reach or view blocked content. Such alternative technologies included all virtual private networks (VPNs) and proxy Web sites used to access such content. However, these measures had been criticized as being technically impossible during the debates before the Omnibus Law was passed by the Turkish Parliament. Many of these critics were proven correct, as access to the banned Web site continued through the use of these alternative methods, with service providers only implementing further

restrictions on some of these methods after it had become apparent that many individuals, including many politicians, were using them to access Twitter.

The court decisions listed by the Directorate as grounds for the blocking order all related to private individuals who had applied for the removal of content on the grounds that the content was violating their personal rights. However, it is important to note that one of the court decisions was issued on February 3, 2014, and was in fact an appeal of an earlier decision made on December 24, 2013, both dates before the amendments of the Omnibus Law came into effect. As stated above, the previously applied provisions of the Internet Broadcast Law did not separately cover the right to personal privacy, but only covered the violation of personal rights in general and granted the court the authority to issue an order blocking the violating content.

The more recent court decisions made after the amendments introduced by the Omnibus Law relate to applications made pursuant to Article 9 and Article 9A of the amended Internet Broadcast Law. As the new provisions allow the complainants to directly apply to the courts for a blocking order without having to contact the content or service provider, it is thought that these complainants made direct application to the relevant courts. However, it is important to note that none of the decisions were for a complete blocking of Twitter, merely the removal or blocking of the specific violating content.

The final decision that was provided as a basis for the blocking of Twitter was the decision made by the Istanbul Chief Prosecutor's Office. However, as per the provisions of the Internet Publication Law, blocking orders can be issued only by a prosecutor in the situation of a catalogue crime, and such decisions must then be approved by a judge within 24 hours. Under the provisions of the current Internet Broadcast Law, prosecutors do not have the authority to make a decision regarding the violation of personal rights or the right to privacy. As the Prosecutor's decision was dated March 20, 2014, it is believed that this final decision was the basis of the blocking order. The Turkish Bar Association announced that this decision made by the prosecutor was invalid and that they had lodged an administrative appeal against the blocking order implemented in accordance with the prosecutor's decision. The general blocking order that blocked access to the entire Web site, rather than the specific violating content also was criticized as the Directorate overstepping its authority and incorrectly applying the provisions of the Internet Broadcast Law.

The initial appeal against the blocking order was made by the Turkish Bar Association through the process of administrative appeal. In the appeal heard before the 15th Ankara Administrative Court, it was argued that such blocking orders must be based on reasoned court decisions and that as none of the court decisions had ruled for a complete block of Twitter, the action taken by the Directorate had gone beyond the scope of authority. The Administrative Court ruled for the issuing of a stay order on the blocking of Twitter, but this order was not immediately implemented by the Directorate as the authorities claimed to have a legally determined period of 30 days in which to implement the ruling of the Court.

A further appeal was made to the Constitutional Court by three separate individuals on the grounds that the blocking of Twitter in its entirety was disproportionate, constituted censorship and was a violation of the constitutional rights of freedom of speech and communication. The applicants also stated that by issuing a complete blocking order, rather than the removal of specific content, the Directorate had gone beyond the scope of its authority. On April 2, 2014, the Constitutional Court ruled in favor of the applicants and decided that the Directorate had to remove the blocking order. Access to Twitter was restored shortly after the decision of the court was reported to the Directorate and the Authority. The full reasoned decision of the Constitutional Court, that heavily cited the constitutional right to freedom of speech and expression, was published in the Official Gazette dated April 3, 2014.

Shortly after the blocking of access to Twitter, on March 27, 2014, the Directorate also banned access to the video sharing Web site Youtube due to the posting of a conversation alleged to have taken place between the Minister for Foreign Affairs and senior members of the Turkish Intelligence Organisation. However, while access was banned to the Web site as per the provisions of the Internet Broadcast Law, the provisions listed as grounds for the blocking order related to Article 8, which grants prosecutors and courts greater authority in cases where one of the crimes listed in the provisions are being investigated or prosecuted.

However, even though Article 8 grants prosecutors and courts such authority, conflicting statements were made as to the specific reason for the implementation of the blocking order. The Minister of Foreign Affairs issued a statement that the blocking order had been due to the protection of national security, whereas the sub-section of the provision listed on the blocking order issued by the Directorate cited crimes against Atatürk. It is important to note that Youtube has been previously blocked in Turkey due to the uploading of content insulting the memory of Atatürk.

Following the decision of the Constitutional Court regarding the blocking order applied to Twitter, an appeal was made to the criminal court that issued the initial blocking order against Youtube. While the court initially removed the blocking order that was applied to the entire Web site, rather than only the offending URL extensions, the general block was reinstated upon appeal by the Prosecutor. Youtube subsequently sought administrative and judicial appeal against the blocking order, citing the disproportionate restriction of freedom of expression. Applications also were made to the Constitutional Court by Youtube and several other individuals on the basis that the blocking of Youtube had infringed on the rights upheld in the Turkish Constitution.

Before the application to the Constitutional Court could be processed, upon further appeal the decision of the court of first instance as based on the appeal of the Prosecutor was declared to be null. This decision was reported to the Directorate, however the Directorate stated that the blocking order on Youtube would still stand as the infringing content had not been removed. The Minister for Transportation and Communication, the Ministry that the Authority is linked to, stated that once all infringing content had been removed, access would be restored. Upon application by Youtube, a stay order also was issued by the administrative courts; but similar to their actions in the example of the blocking of Twitter, the Directorate did not implement this order in a timely manner.

During the appeals process and the applications to the Constitutional Court it was highlighted that in addition to being a restriction on the freedom of speech and expression, the blocking of Youtube in its entirety was contrary to the amended Internet Broadcast Law. The applicants stated that while Article 8 of the Internet Broadcast Law did grant prosecutors and courts to issue blocking orders themselves, the catalogue crimes for which they could issue blocking orders had been stated exhaustively and did not include issues of national security. The applicants argued that extending the blocking order to include the grounds of insulting the memory of Atatürk had been issued in bad faith, in order to qualify the already issued blocking order under the provisions of the Internet Broadcast Law. The applicants also stated that the amended Internet Broadcast Law had determined the norm as only issuing a blocking order against specific pages or sections that featured the offending content, rather than issuing a blocking order against an entire Web site. By continually applying a uniform blocking order against the entire content of Youtube, it was argued that the Directorate had surpassed its scope of authority and had unduly restricted the constitutional right to freedom of expression.

On reviewing the applications made by Youtube and the other individual applications, the Constitutional Court ruled for removal of the blocking order applied to Youtube and the reasoned decision was published in the Official Gazette of June 6, 2014. After notifying the Directorate of this decision of the Constitutional Court, the blocking order implemented against Youtube was finally removed.

CONCLUSION

As illustrated by the initial blocking orders issued against Twitter and Youtube, and the subsequent reluctance of the Directorate to remove these blocking orders despite the ruling of administrative courts, the concerns relating to the amended provisions of the Internet Broadcast Law are not unfounded. Although the legal basis for issuing such blocking orders has been established with the provisions of the amended Internet Broadcast Law, these two examples have shown that prosecutors, courts, and the Directorate in fact may issue orders that go beyond the scope of their established authority.

Issuing blocking orders that go beyond their scope of authority has lead to concerns that the new provisions of the amended Internet Broadcast Law will be used for reasons of political gain and censorship. These concerns were particularly voiced in

relation to the timing of the blocking orders against Twitter and Youtube.

Additionally with the establishment of the Association of Access Providers—an association that is seemingly closely linked to the Directorate—and with the increased obligations placed on content, hosting, and service providers there is an undeniable element of central state control being imposed on the persons engaged in the provision of Internet content and Internet related services. The initial examples of the application of these new provisions have shown that they are susceptible to state and governmental influence and it would be beneficial to Turkey's developing Internet user base if the provisions were revisited in light of the rulings of the Constitutional Court in the Twitter and Youtube cases.

Indeed, the rulings of the Constitutional Court in the Twitter and Youtube cases have indicated a welcome understanding by the Court of the necessities of modern technology and its role in the maintenance of freedom of speech and freedom of expression. Particularly in their ruling on the application relating to the blocking of Youtube, the majority verdict of the Court highlighted that such social media tools were essential for the sharing, spreading, and communication of information and news, and that blocking the entire Web site would affect millions of individual users.