PRIVACY ISSUES IN THE WORLD OF ANTI-DOPING!

DATA PRIVACY ISSUES RELATING TO ANTI-DOPING HAVE BEEN A HOT TOPIC IN THE MEDIA DURING THE LAST FEW MONTHS. THE ISSF IPOD ANSWERS SOME IMPORTANT QUESTIONS FOR ITS READERS ON THIS INCREASINGLY IMPORTANT TOPIC.

QUESTION:
THE MEDIA HAS REPORTED THAT CONFIDENTIAL MEDICAL INFORMATION FROM ATHLETES FROM ALL OVER THE WORLD AND FROM ALL SPORTS WAS LEAKED. WHY AND HOW DID THIS HAPPEN AND WHAT HAS BEEN DONE ABOUT IT SINCE?

ANSWER:
It has been reported in the media and confirmed by the World Anti-Doping Agency (WADA) that on five separate occasions since September 13, 2016, a Russian cyber espionage group operator by the name of Tsar Team (APT28), also known as "Fancy Bear" leaked batches of confidential athlete data from WADA's Anti-Doping Administration and Management System (ADAMS) on its website and to the general media.

WHAT HAPPENED?
As explained by WADA in its various media releases, the group illegally gained access to ADAMS via an International Olympic Committee (IOC)-created account for the Rio 2016 Games. Confined to the Games, the IOC account included such confidential medical data as Therapeutic Use Exemptions (TUE) delivered by International Sports Federations and National Anti-Doping Organizations.

We all know that the TUE process is a means by which an athlete can obtain approval to use a prescribed prohibited substance or method for the treatment of a legitimate medical condition. It is widely agreed that the TUE program is a rigorous and necessary part of elite sport, which has overwhelming acceptance from athletes, physicians and all Anti-Doping stakeholders worldwide.

Therefore, the criminal activity undertaken by the cyber espionage group, which sought to undermine the TUE program and the work of WADA and its partners in the protection of clean sport, has been viewed as a low blow at innocent athletes whose personal data was exposed as a result.

WHY DID IT HAPPEN?
As per its September 14, 2016 media release, WADA has no doubt that these ongoing attacks were being carried out in retaliation against the Agency, and the global Anti-Doping system, because of its independent Pound and McLaren investigations which exposed state-sponsored doping in Russia. WADA condemned this criminal activity and asked the Russian Government to do everything in their power to make it stop as continued cyber-attacks emanating from Russia seriously undermine the work that is being carried out to rebuild a compliant anti-doping program in Russia.

HOW DID IT HAPPEN?
Fancy Bear illegally obtained the data from an account in ADAMS which was created especially for the Rio 2016 Olympic Games (Rio 2016 ADAMS Account); and, therefore, contained information on the TUE history of athletes who participated in the Rio Olympic Games. Access to ADAMS was obtained through spear phishing of email accounts; whereby, ADAMS passwords were obtained enabling access to ADAMS account information confined to the Rio 2016 Games.

A spear phishing email aims to trick the recipient into divulging information, such as their username and password, to gain access to an application of interest

WHAT CORRECTIVE MEASURES WERE IMPLEMENTED TO RECTIFY THE PROBLEM?
Firstly, and perhaps most importantly, it should be noted that the broader ADAMS was not compromised in the attack and continues to be utilized world-wide, without problem, by athletes, Anti-Doping Organizations (such as the ISSF), doping control service providers, accredited-laboratories and WADA.

Upon learning of the incident, WADA promptly formed a multi-disciplinary incident response team, comprised of internal and external resources, including representatives of its IT, legal, and communications teams. The Agency also liaised with leading law enforcement agencies in Canada and elsewhere on all aspects of this investigation, including decisions on taking down information from the Fancy Bear website and other social media sites.

In the interest of keeping stakeholders apprised of its handling of the matter, WADA prepared the following Summary which was published on October 2016. It includes an overview of the incident and outlines actions that the Agency has taken to date to contain the breach.

- In June 2016, WADA created the Rio 2016 ADAMS Account to hold Olympic athlete information required to fulfill the doping control program at the 2016 Olympic Games. Following its creation, the International Olympic Committee (IOC) had full administrative authority over this Account. As administrator of the Account, the IOC created Account credentials for those responsible for running the Anti-Doping program during the Games, including establishing two accounts for WADA representatives, who were part of WADA's Independent Observer ("IO") program for the 2016 Olympic Games.

- Before and during the 2016 Games, third party hackers targeted a number of WADA and IOC email accounts for an email spear phishing attack; which led to the compromise of certain ADAMS passwords.

- WADA's technical and forensic team's current assessment is that an intruder illegally accessed the Rio 2016 ADAMS Account multiple times between August 25, 2016 and September 12, 2016, using credentials unlawfully obtained from one of these targeted users.

- On 13 September, the intruder, calling itself "Fancy Bear," released the first batch of data, comprised of TUE information, on its website. The intruder has since released data related to current and expired TUEs

on five other occasions – always in relation to athletes who competed at the 2016 Olympic Games. The released data all corresponds to the data thefts that occurred between August 25 August and September 12 as described above.

- Upon learning of the intrusion into the ADAMS system on September 13, WADA began taking additional actions that same day to secure the system and contain the known impact of the attack, including:
  - deactivation of all Rio 2016 ADAMS accounts;
  - disabling the self-service "forgot password" reset feature;
  - increasing logging capabilities related to security events;
  - increased monitoring of logs and network activity; and
  - deactivation of dormant accounts.

- WADA also promptly engaged FireEye Inc., d/b/a Mandiant, a premier security and forensic consulting firm, to conduct a thorough and comprehensive investigation of WADA's assets, networks, and systems, including ADAMS, to determine the scope of the intrusion and access to data stored on such systems, as well as to contain any ongoing threat. Mandiant's analysis has been submitted, and it has not found any evidence of additional compromise to ADAMS data beyond the export of the Rio 2016 ADAMS Account data through 12 September, as described above.

- In addition to broad stakeholder and media communications immediately after each leak, WADA contacted all athletes impacted and their Anti-Doping Organizations – both International Federations and National Anti-Doping Organizations – so that they could provide them with the necessary support.

- Moreover, WADA advised all ADAMS users to vigilantly monitor their electronic communications and remain alert for attempted phishing schemes.

WHAT ADDITIONAL MEASURES ARE NOW BEING TAKEN BY WADA TO AVOID THIS FROM HAPPENING AGAIN?

In terms of longer-term actions taken by WADA to further enhance ADAMS security, in addition to implementing additional authentication controls, the Agency is enhancing its security logging and monitoring program and will complete a full assessment to enhance vulnerability and security controls.

The Agency will also provide more guidance to users regarding how they can prevent the inadvertent communication of passwords to third parties who use spearfishing techniques.

FINAL WORDS

Clearly, this was an important data breach that brought the importance of rigorous data privacy regulations and safeguards, notably in the Anti-Doping sphere, to the public eye. WADA will certainly do everything it can to ensure that such a breach never re-occurs.

The creation and respect of data privacy laws is of utmost importance because as a condition to participating in sport, all athletes consent to their data being used, albeit strictly for anti-doping purposes.

Therefore, data privacy laws like the World Anti-Doping Code's International Standard for the Protection of Privacy and Personal Information have been drafted and are regularly amended to strengthen current data privacy regulations and safeguards. The application of this Standard is mandatory for all Signatories under the World Anti-Doping Code. Its procedures must respected and strictly applied by every individual and organization involved in the implementation of the World Anti-Doping program in order to contribute to its success.

We live in a world where everything is computerized and based on electronic data. Thankfully, firewalls, encrypted codes, data protection safeguards and other means of protecting confidential electronic personal data are constantly being created, updated and improved upon in order to ensure the protection and privacy of personal information.

Yet, as WADA has learned the hard way, no computer system is totally immune from hackers.

This is the reality of the world we live in. It is a reality that we must all accept.

QUESTION:

WHAT KINDS OF MEASURES ARE TAKEN BY WADA AND ISSF TO PROTECT THE PERSONAL INFORMATION I PROVIDE DURING DOPING TESTS AND WHEREABOUTS FILINGS?

ANSWER:

There are a variety of safeguards taken to ensure that all relevant parties involved in anti-doping in sport adhere to a set of minimum privacy protections when collecting and using athlete personal information such as information relating to whereabouts, doping controls and Therapeutic Use Exemptions (TUEs).

WADA and all Anti-Doping Organizations, including the ISSF, share responsibility for ensuring that personal information processed in connection with Anti-Doping activities is protected as required by data protection and privacy laws, principles and standards.

To this end, the World Anti-Doping Code (Code) International Standard for the Protection of Privacy and Personal Information (ISPPPI) was developed as a mandatory International Standard of the World Anti-Doping Program.

SHORT LEGISLATIVE HISTORY

The rationale behind the development of the ISPPPI when it was first drafted in 2009 was to ensure that organizations and all individuals involved in Anti-Doping in sport apply appropriate, sufficient and effective privacy protections to personal information that they process, regardless of whether this is also required by applicable laws.

Before it was adopted, a WADA expert reference group reviewed, discussed and prepared the document, and specifically took into account the Organization for Economic Cooperation and Development's (OECD) 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS. No. 108); the APEC Privacy Framework; the Charter of Fundamental Rights of the European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995 on the Processing of personal data and on the free movement of such data, and other international and regional data privacy rules and standards.

The ISPPPI has been updated since it was first adopted (notably in 2015 with the advent of the new World Anti-Doping Code) and remains subject to modification if and when necessary.

PURPOSE AND SCOPE

The World Anti-Doping Code (Code) requires athletes and athlete support personnel to furnish a significant amount of Personal Information to ADOs such as International Federations (in this case the ISSF) and their relevant National Anti Doping Organization.

As a result, it is essential that the ISSF, just like all other ADOs subject to the Code, appropriately protect the personal information that it processes both to meet legal standards as well as to ensure the continued confidence and trust of those involved in organized sport.

The purpose of the ISPPPI is to ensure that Anti-Doping Organizations such as the ISSF apply appropriate, sufficient and effective privacy protections to the personal information they process when conducting Anti-Doping programs, in recognition of the fact that personal information gathered in the Anti-Doping context can impinge upon and implicate the privacy rights of persons involved in and associated with organized sport.

The Code and the ISSF Anti-Doping Rules recognize and reiterate the importance of ensuring that the privacy rights of persons subject to anti-doping programs based on the Code are fully respected. In support of this commitment, the ISPPPI provides mandatory rules and standards relating to the protection of personal information.

As a Code Signatory, the ISSF respects and implements the ISPPPI and conforms to all its principles when collecting and handling personal information pursuant to the Code and its ISSF Anti-Doping Rules.

HOW DOES THIS APPLY TO THE ISSF?

As previously stated, the ISSF adopts, respects, and fully complies with the ISPPPI.

Because the ISPPPI requires personal data to be collected and processed on the basis of consent, or another legal basis, the ISSF has

made it clear both in the ISSF Anti-Doping Rules Ðwhich all ISSF athletes agree to comply with as a matter of eligibilityÐ as well as the Athlete Declaration Ðwhich all athletes agree to as a condition of obtaining an ISSF ID NumberÐ that all athletes consent to the ISSF's usage of their information; so long as this information is used in accordance with the ISPPPI and any other applicable data privacy laws.

Specifically, the ISSF respects the ISPPPI principles with regards to personal information. Personal information is defined as including, but not being limited to, information relating to an athlete's name, date of birth, contact details and sporting affiliations, whereabouts, designated therapeutic use exemptions, anti-doping test results, and results management (including disciplinary hearings, appeals and sanctions).

Personal information also includes personal details and contact information relating to other persons, such as medical professionals and other persons working with, treating or assisting an athlete in the context of anti-doping activities. Such information remains personal information and is regulated by the ISPPPI and by reference, the ISSF Anti-Doping Rules for the entire duration of its processing, disregarding if the relevant individual remains involved in organized sport.

The ISSF also fully complies with the ISPPPI with regards to sensitive personal information. Sensitive personal information is defined as personal information relating to a participant's racial or ethnic origin, perpetration of offences (criminal or otherwise), health (including information derived from analyzing an athlete's samples or specimens) and genetic information.

FOR EASE OF REFERENCE, THE RELEVANT PORTIONS OF THE 2017 ISSF ANTI-DOPING RULES READ AS FOLLOWS:

ARTICLE 5
TESTING AND INVESTIGATIONS
(…)

5.1.4 The handling and retention of any data or information or intelligence collected in the course of the ISSF testing program and/or in accordance with the ISSF test distribution plan shall respect and comply with the International Standard for the Protection of Privacy and Personal Information.

ARTICLE 15
CONFIDENTIALITY AND REPORTING
(…)

15.6 DATA PRIVACY

15.6.1 The ISSF may collect, store, process or disclose personal information relating to Athletes and other Persons where necessary and appropriate to conduct their anti-doping activities under the Code, the International Standards (including specifically the International Standard for the Protection of Privacy and Personal Information) and these Anti-Doping Rules.

15.6.2 Any Participant who submits information including personal data to any Person in accordance with these Anti-Doping Rules shall be deemed to have agreed, pursuant to applicable data protection laws and otherwise, that such information may be collected, processed, disclosed and used by such Person for the purposes of the implementation of these Anti-Doping Rules in accordance with the International Standard for the Protection of Privacy and Personal Information and otherwise as required to implement these Anti-Doping Rules.

And

Point 4 of the 2017 **Athlete Declaration** reads: "I agree and consent to the ISSF collecting, processing, disclosing and using information for the purposes of the implementation of the ISSF Anti-Doping Rules in accordance with the International Standard for the Protection of Privacy and Personal Information and pursuant to applicable data protection laws."

SUMMARY

As a condition of participation in Shooting Sport, all ISSF athletes agree and consent to sharing their personal information, sometimes sensitive, in the course of the mandatory ISSF anti-doping activities and procedures.

Still, all ISSF athletes can rest assured knowing that the ISSF, their NADO and anyone involved in carrying out the World Anti-Doping program is subject to the same set of rigorous ISPPPI data privacy rules.

To summarize, all ISSF athletes can rest assured that any personal and sensitive information they share as a condition to and by virtue of participation in Shooting Sport is being protected by a variety of unyielding privacy safeguards.

Thank you for reading the IPOD in 2016. We will be back in 2017 with our 2016 Anti-Doping Report summarizing all of ISSF Anti-Doping activities throughout the year.

Janie Soublière BSS. LLM. LLB.
ISSF Counsel and Consultant Anti-Doping in Sport