BUSINESS INSURANCE

People

How a misunderstanding of GDPR could heighten cyber exposure

Richard M. Borden and Joshua A. Mooney

February 03, 2019

Richard M. Borden, left, and Joshua A. Mooney

Cyber vulnerabilities and incidents are rarely organization-specific. A security breach into one organization's network can provide hackers with the ability to breach another organization's network by using the same tactics, techniques and procedures. Thus, a security breach into one organization may initiate a chain of security breaches compromising multiple networks of numerous organizations. Threat information sharing can short-circuit, if not prevent, chain security breaches by providing real-time information to patch vulnerabilities and thwart further attacks targeting those vulnerabilities.

However, a critical misunderstanding has stifled this efficient and cost-effective means to combat cyberattacks, which in turn may be causing real and long-lasting damage. The General Data Protection Regulation is intended to protect the fundamental rights of EU individuals, called data subjects in the EU. However, GDPR has led some to question whether threat information sharing is permissible under the regulation, notwithstanding that sharing threat information advances fundamental tenets of GDPR for the protection of personal data and privacy as a fundamental right. This uncertainty is not an academic question. It potentially has deprived organizations, including banks, brokerages, insurance companies and other critical infrastructure, of an essential tool to both better protect their network and consumers from cyber crime and comply with regulatory requirements for effective data security.

The short answer is that threat information sharing can be lawful. Organizations, including Information Sharing Analysis Centers, or ISACs, should look to Article 6(1)(f) of GDPR to model information-sharing programs. (Privacy notices can account for transparency requirements under Articles 13 and 14.) In fact, Financial Services Information Sharing Analysis Center, or FS-ISAC, has led the way with this analysis in a recent white paper.

Article 6(1)(f) of GDPR states that processing personal data is lawful when it "is necessary for the purpose of the legitimate interests pursued by the controller [loosely, the organization collecting the information] or by a third party." The inclusion of third-party interests is critical.

The effect is that the interests of the organizations combating cyber risks, as well as the interests of governments, persons and the general public at large, are all relevant for determining the lawfulness of the processing. Establishing lawfulness of processing personal data must meet a three-step test: legitimacy, necessity and a balancing of interests.

Legitimacy: As described in the Article 29 Working Party, or A29WP, guidance on legitimate interests, Opinion 06/2014, an entity can establish "legitimacy" of the interests being served by showing that its conduct is lawful, clearly articulated, and real and present (i.e., not speculative). Organizations such as ISACs can demonstrate legitimacy of interests in sharing threat information when taken under a legal directive, such as for public welfare, and when using internal confidentiality controls to help meet Article 6's balancing test, discussed further below. Organizations should have little difficulty demonstrating the third prong: Cyberattacks and the interests to thwart them are real and present.

Necessity: An entity may establish "necessity" by showing that the processing of personal data is necessary and proportionate to the pursuit of the legitimate interest. To be necessary, sometimes referred to as "strictly necessary," there must be no viable or practical alternative method to achieve the purpose behind the interest. For example, the organization sharing threat information should confirm that it cannot achieve the goal of sharing the threat information (i.e. data and network security, and the prevention of fraud) in a more obvious or less intrusive way. This should be an easy test. Sharing certain personal data such as IP or email addresses can be essential for rapidly identifying and preventing chain security breaches and further exploitation of discovered network vulnerabilities in organizations. Information sharing also can prevent further crime against an individual whose data is stolen. An organization may show proportionality by the impact of the processing on the individual whose personal data is shared. The balancing test discussed below is an effective tool to demonstrate that proportionality.

Balance: The Article 6(1)(f) balancing of interests weighs the legitimate interests of the entity collecting and analyzing the information, or the interests of a third party, against the interests and fundamental rights of the individual whose data is processed. In the context of threat information sharing, the purpose and interest behind threat information sharing should not be outweighed by the individual's interests. Threat information sharing is not arbitrary or punitive. It is done with specific goals of network security, and to prevent fraud and crime, with the ultimate effect of protecting persons from harm. For instance, the processing of stolen/ victim personal data to prevent further fraud against that person would not be outweighed by the individual's interests because such processing would advance the person's interests by preventing further harm, or him or her, to validate a loss to provide an opportunity for recovery. The interests of the threat actors also would not override the processing of personal data, because such processing should not be disproportionate to the threat actor's rights and freedoms. Although the processing could lead to legal actions taken against the threat actor, including incarceration, threat actors do not have the right to evade justice, and the administration of justice would have its owns checks and balances to ensure proportionality.

Hopefully, the contention that GDPR does not permit threat information sharing is exposed as a misunderstanding. Threat information sharing is an essential tool in cybersecurity arsenal that enables organizations to achieve the very goals GDPR is intended to advance: data security and individual privacy.

Richard M. Borden is partner and chief privacy officer with White and Williams LLP. He can be reached at 212-631-4439 or bordenr@whiteandwilliams.com. Joshua A. Mooney is partner and co-chair of the cyber law and data protection group with White and Williams LLP. He can be reached at 215-864-6345 or mooneyj@whiteandwilliams.com.