Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 1** **January 2022**

Editor's Note: Private Public Relations?
Victoria Prussen Spears 1

Can Public Relations Be Private? The Attorney-Client Privilege and Communications with Public Relations Firms
Carl H. Loewenson, Jr., and Lauren S. Gonzalez 3

Commerce Department Issues Long-Awaited Rule on Cybersecurity, Hacking Tools
Lori E. Scheetz, John R. Shane and Nazak Nikakhtar 13

Significant Impact on Personal Data Transfers Due to the New Standard Contractual Clauses and Final Guidance on Supplementary Measures
Natasha G. Kohne, Michelle A. Reed, Jenny Arlington, Rachel Claire Kurzweil, Jay Jamooji and Sahar Abas 18

Australian Privacy Overhaul on the Horizon
Sophie Dawson and Emma Croft 26

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [1] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Pratt's Privacy & Cybersecurity Law Report
January 2022

Editor's Note
Private Public Relations?

Victoria Prussen Spears*

Welcome to the January 2022 issue of *Pratt's Privacy & Cybersecurity Law Report*! This issue rings in the New Year with a variety of timely, important articles. We begin with an article discussing privacy and public relations.

Can Public Relations Be Private?

In our lead article, "Can Public Relations Be Private? The Attorney-Client Privilege and Communications with Public Relations Firms," Carl H. Loewenson, Jr., a partner at Morrison & Foerster LLP, and Lauren S. Gonzalez, who was a summer associate at the firm, explain that although broad claims of attorney-client privilege for communications with public relations companies have not been successful, limited claims of work product privilege have been accepted.

Cybersecurity

Next, Lori E. Scheetz, John R. Shane and Nazak Nikakhtar, partners at Wiley Rein LLP, review the elements of an interim final rule published by the Bureau of Industry and Security of the U.S. Department of Commerce that establishes controls on certain cybersecurity items designed to curtail exports of hacking tools to China, Russia and other countries that may use such items for malicious purposes in their article, "Commerce Department Issues Long-Awaited Rule on Cybersecurity, Hacking Tools."

* Victoria Prussen Spears is a writer, editor, and law firm marketing consultant for Meyerowitz Communications Inc. A graduate of Sarah Lawrence College and Brooklyn Law School, Ms. Spears was an attorney at a leading New York City law firm before joining Meyerowitz Communications. Ms. Spears, who is Editor of *The Banking Law Journal*, *Pratt's Journal of Bankruptcy Law*, *Pratt's Energy Law Report*, *Pratt's Government Contracting Law Report*, and *Pratt's Privacy & Cybersecurity Law Report*, all published by Lexis, can be reached at vpspears@meyerowitzcommunications.com.

Personal Data Transfers

Natasha G. Kohne, Michelle A. Reed, Jenny Arlington, Rachel Claire Kurzweil, Jay Jamooji and Sahar Abas, attorneys at Akin Gump Strauss Hauer & Feld LLP, contributed an article titled "Significant Impact on Personal Data Transfers Due to the New Standard Contractual Clauses and Final Guidance on Supplementary Measures," in which they set out the key features of the updated standard contractual clauses for controllers and processors and the European Data Protection Board's finalized recommendations on the use of supplementary measures.

Privacy in Australia

In our next article, "Australian Privacy Overhaul on the Horizon," Sophie Dawson and Emma Croft, attorneys at Bird & Bird, discuss a proposed privacy code that, if implemented, would have a fundamental impact on the reach, enforcement risk and effect of Australian privacy laws.

Enjoy the issue and have a very Happy and Healthy New Year!

Can Public Relations Be Private? The Attorney-Client Privilege and Communications with Public Relations Firms

By Carl H. Loewenson, Jr., and Lauren S. Gonzalez*

In this article, the authors explain that although broad claims of attorney-client privilege for communications with public relations companies have not been successful, limited claims of work product privilege have been accepted.

Open *The New York Times* or *The Wall Street Journal* website on any given day, and odds are you will find a report of a data breach or a ransomware attack. According to a recent report, by October 2021 there were already more reported data breaches than in all of 2020.[1] Since data breaches tend to rise in the last quarter of the year, 2021 may surpass the all-time high of 1,529, set in 2017. While not all of these breaches get front-page attention, many of these incidents – particularly those involving the exfiltration of millions of customers' sensitive data – lead to sustained press attention, as regulators investigate the incidents and civil lawyers file lawsuits ranging from consumer class actions to securities class actions and corporate derivative lawsuits.

Attorneys representing a company that has suffered a data breach or ransomware attack therefore find themselves handling problems that are often not confined to legal risks. Faced with sudden and unwelcome media interest, companies without a robust in-house public relations ("PR") group will for many good reasons want to retain a public relations firm. While there is a body of literature in public relations and academic circles arguing that public relations may have become an integral part of the lawyer's role in high-profile matters, the work an attorney does in pursuit of that role may not be covered by the attorney-client privilege. If a lawyer believes that hiring a public relations firm or consultant would further the client's litigation interests, the lawyer should not assume those communications will be covered by attorney-client privilege or work product protection.

Two cases in the early 2000s from the U.S. District Court for the Southern District of New York, *In re Grand Jury Subpoenas Dated Mar. 24, 2003 Directed to (A) Grand Jury Witness Firm & (B) Grand Jury Witness*[2] ("*In re Grand Jury*") and *In re Copper Mkt.*

---

* Carl H. Loewenson, Jr. (cloewenson@mofo.com), a partner in the New York City office of Morrison & Foerster LLP, is a member of the firm's Securities Litigation, Securities Enforcement and Investigations + White-Collar Defense groups. His practice focuses primarily on white-collar defense, including regulatory matters. Lauren S. Gonzalez was a summer associate at the firm.

[1] *See* https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks/ (last visited Oct. 22, 2021).

[2] *In re Grand Jury Subpoenas Dated Mar. 24, 2003 Directed to (A) Grand Jury Witness Firm & (B) Grand Jury Witness*, 265 F. Supp. 2d 321 (S.D.N.Y. 2003).

Antitrust Litig.[3] ("*In re Copper*"), extended attorney-client privilege to communications with public relations consultants made for the purpose of informing the legal advice the lawyers provided to their respective clients. Though still good law, New York courts – state and federal – consistently construe the holdings narrowly. When rejecting application of these holdings to subsequent public relations cases, courts stress the context and fact-specific nature of the inquiry as well as the precedents' unique contexts.

The decision by Judge Lewis Kaplan in *In re Grand Jury* held that attorney-client privilege covered communications with the public relations firm hired by the legal team representing the target of a high-profile federal criminal investigation. The consultants were tasked to help counter the growing public pressure on prosecutors to indict. The court found that the firm's work differed from typical publicity campaigns: their audience was not the general public, but the government actors responsible for charging decisions. The specific litigation goal the team was tasked with, avoiding an indictment or limiting the scope of one, "promote[d] broader public interests in . . . the administration of justice."[4]

The decision by Judge Laura Swain in *In re Copper* also protected communications between counsel and a public relations firm because the PR firm was determined to be the "functional equivalent" of the client's employee.[5] When a foreign corporation, whose principals did not speak English well and lacked experience in dealing with the Western media, suddenly became involved in a high-profile litigation, they hired the PR firm. The public relations firm worked in the corporation's office and possessed authority to make decisions on behalf of the foreign corporation concerning its public relations strategy. Finding that the firm was "essentially, incorporated into [the foreign corporation]'s staff to perform a corporate function that was necessary in the context of the government investigation," the court determined that the consultant's communications with counsel were protected like a corporate employee's communications would be.[6]

These cases have proven to be the exception to the rule. As a later Southern District of New York decision*, Haugh v. Schroder Inv. Mgmt. N. Am. Inc.*,[7] by Judge Denise Cote explained when denying privilege to a third-party PR consultant, "[s]ome attorneys may feel it is desirable at times to conduct a media campaign, but that decision does not transform their coordination of a campaign into legal advice." In order to have communications with PR firms or consultants covered by attorney-client privilege, the party asserting the privilege must demonstrate the necessity of their services for providing legal advice. The party asserting privilege must show that there is a nexus between the consultant's work and how it affects and assists the lawyers in the litigation or investigation.

---

[3] *In re Copper Mkt. Antitrust Litig.*, 200 F.R.D. 213 (S.D.N.Y. 2001).

[4] *In re Grand Jury*, 265 F. Supp. 2d at 329 (quoting *Upjohn Co. v. United States*, 499 U.S. 383, 389 (1981)).

[5] *In re Copper*, 200 F.R.D. at 220.

[6] *Id.* at 219.

[7] *Haugh v. Schroder Inv. Mgmt. N. Am. Inc.*, 02 Civ. 7955 (DLC) (S.D.N.Y. Aug. 25, 2003).

Shortly before *In re Grand Jury* and *In re Copper*, Judge Jed Rakoff in the Southern District of New York, in *Calvin Klein Trademark Trust v. Wachner*,[8] had declined to protect as privileged certain communications between a company and its PR firm, because the PR firm was providing typical public relations advice such as reviewing press coverage and reaching out to various reporters rather than informing the legal strategy. If the public relations consultants provide more typical public relations functions or advice for communication with the general public and media, courts often find that the reasoning in *Calvin Klein* controls. New York state privilege law is more conservative than federal privilege law and requires an even higher showing: that the third party "be nearly indispensable or serve some specialized purpose in facilitating the attorney-client communications."[9] Although broad claims of attorney-client privilege for communications with PR companies have not been successful, limited claims of work product privilege have been accepted.

"NECESSARY" DEFINED

Courts applying federal common law require that the party claiming privilege must demonstrate the PR firm was necessary for the lawyers to provide legal advice to their client and for the client to obtain legal advice from the attorney. When evaluating whether communications with PR firms should receive attorney-client privilege protections, courts emphasize the unusual circumstances present in *In re Grand Jury*. While accepting that applying privilege for that relationship may have been necessary for the unique context – a high profile criminal investigation where the lawyers were trying to counteract "the broad power of the government" – later courts have not been willing to extend the privilege to lower profile or lower risk situations.[10] Some found the holding almost exclusively "limited by its context: the . . . narrow scenario of public relations consultants assisting lawyers during a high profile grand jury investigation."[11]

The PR firm's role within the attorney-client relationship must be crucial and "beyond the expertise of counsel."[12] In other words, if the consultant does not provide specialized knowledge that the attorneys could not have acquired or understood on their own or directly through the client, there is no privilege. This reasoning is an extension of the holding of *United States v. Kovel* in which the U.S. Court of Appeals for the Second Circuit likened the communications made between the client and an accountant employed by the client's attorney to those between the client and a translator.[13] The court found the privileged relationship extended to parties serving an interpretive function for the client and attorney for concepts the counsel need to comprehend in order to provide legal advice.

---

[8] *Calvin Klein Trademark Trust v. Wachner*, 198 F.R.D. 53 (S.D.N.Y. 2000).

[9] *Egiazaryan v. Zalmayev*, 290 F.R.D. 421, 432 (S.D.N.Y. 2013).

[10] *In re Grand Jury*, 265 F. Supp. 2d at 330.

[11] *Ravenell v. Avis Budget Grp., Inc.*, 08-CV-2113 (SLT) (SMG) (E.D.N.Y. Apr. 4, 2012).

[12] *In re Grand Jury*, 265 F. Supp. 2d at 330.

[13] *United States v. Kovel*, 296 F.2d 918, 921 (2d Cir. 1961).

For example, in a trademark infringement case, *Universal Standard Inc. v. Target Corp.*,[14] the court did not extend attorney-client privilege to the PR firm because they were not utilized in a specific litigation strategy that required the PR firm's help. Nor did the attorneys need public relations employees to act as a translator or interpreter of client communications. In that case, the court found that even without the publicity team the client could have communicated with counsel about the propriety of issuing a press release around the lawsuit's filing.

New York State courts or federal courts with diversity jurisdiction apply New York privilege law, which is more limiting than federal law in extending privilege to third parties. In addition to what federal privilege law requires, courts applying New York law analyze if disclosure to the third party was more than useful or convenient "but nearly indispensable" to facilitate legal advice.

In *Egiazaryan*, for example, the court explicitly distinguished the goals pursued by the public relations firm's activities which were "aimed at burnishing Egiazaryan's image" from the litigation goals which related to the administration of justice in *In re Grand Jury*.[15] The PR firm's insertion into the "legal decision making process" does not create a privileged relationship – no matter how extensive their involvement – if it is not necessary for the client to obtain legal advice "from his actual attorneys."[16]

Fine v. ESPN, Inc.,[17] exemplifies the high burden New York law requires to invoke the agency exception regarding waiver of the privilege as well as the narrow interpretation of *In re Grand Jury*. *Fine*'s facts were closely analogous to those in *In re Grand Jury* – the party claiming privilege over communications with the PR firm was subject to intense and high-profile media scrutiny as well as potential criminal charges. Even though counsel relied heavily on *In re Grand Jury* to argue that the PR firm helped counsel "shape media coverage to avoid prosecution," the court found all but two communications were ineligible for protection because they didn't have anything to do with legal advice.[18]

In a recent case, *People v. Ackerman McQueen*,[19] in the course of a high profile investigation of the National Rifle Association ("NRA") by the New York Attorney General, the NRA argued that communications with its longtime media firm, which had managed NRA platforms and had its employees appear on NRA TV, should be protected by attorney-client privilege. Applying the "necessary" test, the state court in Manhattan explained that the NRA did not need its PR firm to act as a "translator" for the NRA to understand its own lawyer's advice about the Second Amendment – it was a language the lawyers understood.

---

[14] *Universal Standard Inc. v. Target Corp.*, 331 F.R.D. 80 (S.D.N.Y. 2019).

[15] *Egiazaryan*, 290 F.R.D. at 432.

[16] *Id.*

[17] *Fine v. ESPN, Inc.*, 5:12-CV-0836 (LEK/DEP) (N.D.N.Y. May. 28, 2015).

[18] *Id.*

[19] *People v. Ackerman McQueen,* 125 N.Y.S.3d 838 (N.Y. Sup. Ct. 2020).

On the other side of the dynamic, when the media company's employees appeared on NRA TV, the publicists were not necessary to convey legal strategy from the NRA's lawyers. The NRA or one of its employees could tell the publicity company's employee what to say without ever providing legal advice.

PURPOSE OF THE RELATIONSHIP OR COMMUNICATION

Many cases have held that if the publicity specialists are not retained for, or do not provide, necessary assistance for the lawyer's litigation strategy or legal advice, there is no attorney-client privilege. Courts analyzing the applicability of *In re Grand Jury* highlight the specific litigation tasks the counsel needed the PR team to accomplish in order to advance the client's litigation goals, such as "reducing public pressure on prosecutors and regulators to bring charges."[20] The more the publicity work resembles traditional PR tasks for business concerns, the more likely the communications will be not protected under the reasoning of *Calvin Klein*.

Courts look beyond affidavits or engagement letters proffered by those asserting a special or litigation-oriented relationship with PR consultants to determine the nature of the communications and relationship. Some courts deny the privilege after analyzing the nature of the work performed by the consultant.

For example, though the retention letter in *Haugh* stated that the PR consultant, who was also a lawyer licensed in Texas, would "provide us advice to assist us in providing legal services to Ms. Haugh," the court found the services provided by the consultant were "standard public relations services" that were not necessary in the attorney's provision of legal advice to the client.[21]

In *Ackerman McQueen*, the NRA argued that its decades-long relationship with its public relations firm was special and exceeded standard public relations work. The court found that though the firm managed the NRA media platforms and website, administered NRA TV, handled branding and strategy, and entered into contracts on behalf of the NRA, those services did not change the relationship from that of a third-party public relations firm. In another case, the court concluded that drafts exchanged and communications relating to a proposed press release were not for the predominant purpose of seeking or conveying legal advice, so copying the PR consultant on emails about the press release waived any privilege.[22]

General public relations advice strategizing about the effects of the litigation on the client's customers, the media, or on the public generally is not protected. For example, *Breest v. Haggis*,[23] a #MeToo case which garnered considerable media attention, held

[20] *McNamee v. Clemens*, No. 09 CV 1647 (SJ) (CLP) (E.D.N.Y. July 31, 2013).
[21] *Haugh, supra* n.7.
[22] *Pearlstein v. BlackBerry Ltd.,* 13-CV-07060 (CM)(KHP) (S.D.N.Y. Mar. 19, 2019).
[23] *Breest v. Haggis*, 64 Misc. 3d 1211(A) (N.Y. Sup. Ct. 2019).

that attorney-client privilege did not cloak communications from the client, directly or through attorneys, with the PR firm made for the predominant purpose of spinning the information in the media or for business purposes.

Additionally, communications about a litigation strategy that is driven by publicity opportunities for the benefit of the client's image and reputation are not protected. For example, in *McNamee*, the client's legal team's discussion regarding strategic times for filings were driven by trying to get favorable magazine and TV interview profiles and not protected by privilege. PR assistance aimed at communicating with the public at large, even about the legal issues in the litigation, has repeatedly not been granted privilege protection.

Courts also look to the nature of the attorney's role within the dynamic. Federal and state courts have noted that when a lawyer's efforts are concentrated in media and public relations, lobbying, and political activism, then the privilege does not extend to communications with respect to many of those activities. Extending that reasoning, *Gottwald v. Sebert*,[24] a case which involved the famous singer Kesha, held that, in order to be protected from disclosure, the "predominant purpose" of a communication with a PR firm must involve legal advice. The court found that her attorney's communications with a PR firm strategizing a media campaign designed to pressure the litigation adversary into settling quicker and so that the prospective jury pool would be more favorable for the defendant did not satisfy the standard. Communications designed to effectuate these legal objectives, but for reasons not related to the legal merits (like settling out of fear of negative publicity or the prospect of decimating a person's career), did not pass the "predominant purpose" test.

Interposing a law firm in the middle of communications between a PR and its client will not protect the communications from disclosure. In *NXIVM Corp. v. O'Hara*,[25] the court determined from the record that the attorney never used the PR firm's services – hiring them was "a façade. . . . [Counsel] and his law firm were used as intermediaries in name only – a mule – with the anticipated effect of concealing all conversations and all actions under the cloak of an attorney-client privilege or work product."

WORK PRODUCT PROTECTION

Even if the attorney-client privilege has been waived, communications with PR firms may still be protected under the work product doctrine. In order for a communication to qualify as work product, the threshold test requires that (1) the document was drafted in anticipation of litigation or to have an impact on litigation strategy, and (2) it would not have been prepared in essentially similar form irrespective of the litigation. Both elements must be met to warrant protection.

---

[24] *Gottwald v. Sebert*, 58 Misc. 3d 625, 627 (N.Y. Sup. Ct. 2017), *aff'd,* 161 A.D.3d 679 (2018).

[25] *NXIVM Corp. v. O'Hara*, 241 F.R.D. 109, 140 (N.D.N.Y. 2007).

In *Pearlstein*, the court found that a near final version of a press release satisfied the first prong, but not the second, and therefore required its disclosure. Work product protection analysis is an individualized determination depending on the particular facts and circumstances – and sometimes document by document – of the case. Courts require detailed privilege logs and often *in camera* review.

When analyzing whether a communication is work product worthy of this protection, courts require more than a showing that the material was prepared at the behest of a lawyer or provided to one. Just like attorney-client privilege, general public relations advice strategizing about the effects of the litigation on the public, media or business are not protected – the protection is reserved for strategizing about the conduct of the litigation itself. Even if the communications sought "played an important role in [the] litigation strategy," but focused on the former, it will not get cloaked with work product protection.[26]

As a rule, waiver of work product protection is much more difficult to establish than attorney-client privilege waiver. If the publicity-related work product was drafted by counsel or the documents implicitly reflect attorney work product, i.e., witness interview notes written by attorneys, the communication is more likely to be protected than if written by the publicist. Work product disclosed to a PR firm sharing a common interest with the client will stay protected as long as the consultants intend to keep the information in confidence. But a PR firm's release of otherwise protected work product to the media will vitiate the protection. For example, in *O'Hara*, the court found that because work product was disclosed to the PR firm with the expectation that it would be released publicly, that work product did not receive protection.

COUNSEL'S ETHICAL CONSTRAINTS AND DUTIES

Counsel, especially defense counsel, can be faced with competing and seemingly incompatible obligations between codes of professional conduct and the best interests of their client in obtaining the best possible publicity. Traditionally, the role of lawyers and their role as it relates to influencing public opinion was construed narrowly and proscribed extrajudicial statements that could influence jury pools. The use of a PR firm to generate sympathetic media coverage in an effort to influence a prosecutor not to indict is all well and good (and is likely privileged under *In re Grand Jury*); but an effort to generate similar media coverage post-indictment in an effort to influence the trial jury would collide head on with the attorney's ethical obligations.

In New York, the central rule regarding lawyers communicating with the press is Professional Conduct Rule 3.6(a):

> A lawyer who is participating in or has participated in a criminal or civil matter shall not make an extrajudicial statement that the lawyer knows or reasonably should

[26] *McNamee*, *supra* n.20.

> know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

A lawyer also cannot evade this rule by delegating the task to the PR firm. Under Rule 5.3(b), a lawyer is responsible for conduct of a nonlawyer retained by the lawyer that would be a violation of the Rules if engaged in by the lawyer.

While codes of professional conduct now allow for counsel to comment in response to public statements – "limited to such information as is necessary to mitigate the recent adverse publicity" – in order to protect their client's interests, Rule 3.6(d), case law has shifted towards a more liberal view of a lawyer's relationship with the media. Justice Kennedy acknowledged the lawyer's role advocating for his or her client more broadly in the realm of public opinion, explaining in a concurring opinion, "[a]n attorney's duties do not begin inside the courtroom door."[27]

Calvin Klein and *In re Grand Jury* and their progeny both began at this evolved understanding of what is considered an acceptable scope of behavior for a lawyer outside of the courtroom. Though *In re Grand Jury* and *In re Copper* remain the only cases extending the attorney-client privilege to communications made for public relations goals, *Calvin Klein* in rejecting the application of the privilege accepted "that the modern client [may] come[] to court as prepared to massage the media as to persuade the judge."[28]

Although New York courts are not extending attorney-client privilege for communications discussing a strategy aimed at the general public or media, courts are also not sanctioning attorneys for engaging in that conduct. The principle underlying Rule 3.6 is protecting the right to a fair trial. Therefore, pre-indictment counsel partnerships with public relations firms as in *In re Grand Jury* and *Fine* are unlikely to run afoul of the rule. The comments to the New York rule explain that some trials, i.e., criminal jury trials, are the most sensitive to prejudicial extrajudicial speech, whereas non-jury hearings and arbitration proceedings may be less susceptible to prejudice. The judge's comments in *Gottwald*, regarding an email revealing that the attorney had targeted the potential judges and jury pools in his media strategy are illustrative for these distinctions:

> Leaving aside the jury selection implications of such a strategy, it is the duty of this court to render decisions purely based on its views of the correct legal result, without regard to any public relations implications. It would behoove counsel to focus more on persuading this court than the court of public opinion.[29]

---

[27] *Gentile v. State Bar*, 501 U.S. 1030, 1043 (1991).

[28] *Calvin Klein Trademark Trust*, 198 F.R.D. at 56.

[29] *Gottwald*, 58 Misc. 3d at 636, n.11.

FUNCTIONAL EQUIVALENT

If a public relations firm or other consultant is determined to be the "functional equivalent" of the client's employee, then attorney-client privilege will extend to the PR specialists just as it would if they were actually the client's employees. Courts have identified the following non-exhaustive factors, many of which were present in *In re Copper*, which best position companies to meet the functional equivalent test: if the PR firm has primary responsibility for a key corporate job; has a continual and close working relationship with the company's principals on matters critical to the company's position in litigation; and possesses information possessed by no one else at the company.

Other factors include whether the consultant:

- Exercised independent decision-making on the company's behalf or if important aspects of the work were supervised by the client;
- Served as a company representative to third parties;
- Maintained an office at the company or otherwise spent a substantial amount of time working for it; and
- Exclusively worked for the client.

Ackerman McQueen demonstrates the high standard litigants must meet to claim attorney-client privilege under the functional equivalent theory. The NRA's decades-long and relatively involved relationship with the media company did not suffice. Pointing to the fact that the public relations firm had additional clients, its own legal counsel, and negotiated the contract for their employee publicists who appeared on NRA TV, the court also found that the firm never assumed the functions or duties of an NRA employee.

PRACTICE NOTES

While many of the cases that assess the attorney-client privilege and work product protection for communications involving public relations often turn on their facts, a number of themes emerge from the cases of the past two decades. These themes can serve as practice pointers for any counsel considering adding a PR firm to the team in the representation of a client in a high-profile criminal or civil matter.

- The attorney, not the client, should contract with the consultant and be invoiced for services. If relevant, the legal-related work should be kept separate and billed separately from the general PR work. For example, if the same PR firm is assisting with matters related to the conduct of the litigation and also providing assistance in managing the effects of the litigation, separate bills could be beneficial.

- The engagement letter should describe the work as facilitating legal services and should explain the particular project or litigation the consultants are working on as opposed to the company's media image generally.

- If possible, the engagement letter should include a confidentiality clause – similar to the clause that counsel would include in the retention of any consulting expert – and subsequently exchanged documents and emails should include language that recipients should limit dissemination.

- All communications by the client with the consultant should involve an attorney if possible. Though this is not dispositive, it is a relevant factor supporting protection of the communications. An attorney should be copied on all communications with the PR firm.

- When hiring a PR consultant, an attorney should be strategic in the timing of the hire and the type of a consultant. If a PR firm is hired before litigation is reasonably anticipated, it could appear they were employed for more of a business purpose than a litigation one. Additionally, the consultant should ideally be specialized either in crisis work, legal issues, or a particular subject matter that is unfamiliar to the client and attorney.

- Discuss the legal implications of public relations issues in the documents. For example, if the document outlines talking points or a press release, the attorney's comments and edits should state or demonstrate the attorney's considerations of legal impacts of alternative expressions.

Commerce Department Issues Long-Awaited Rule on Cybersecurity, Hacking Tools

By Lori E. Scheetz, John R. Shane and Nazak Nikakhtar*

The authors review the elements of an interim final rule published by the Bureau of Industry and Security of the U.S. Department of Commerce that establishes controls on certain cybersecurity items designed to curtail exports of hacking tools to China, Russia and other countries that may use such items for malicious purposes.

The U.S. Department of Commerce's Bureau of Industry and Security ("BIS") has published[1] a long-awaited interim final rule that establishes controls on certain cybersecurity items designed to curtail exports of hacking tools to China, Russia and other countries that may use such items for malicious purposes. The interim rule also creates a new license exception for Authorized Cybersecurity Exports ("ACE"). The purpose of the interim rule, according to the Commerce Department, is to "help ensure that U.S. companies are not fueling authoritarian practices," such as the use of technology to abuse human rights or conduct other nefarious cyber activities.

The rule follows a spate of hacking incidents[2] and stems from a controversial BIS2015 proposal[3] that was criticized by industry as potentially undermining cybersecurity research and innovation. BIS seeks to address these practical concerns in the interim rule and is requesting public comments on the projected impact of the rule on industry

---

* Lori E. Scheetz, a partner in Wiley Rein LLP, represents U.S. and international clients on export compliance and national security matters, with a focus on U.S. export controls and economic sanctions. John R. Shane, a partner in the firm, represents clients on international trade issues, such as export controls, the Foreign Corrupt Practices Act ("FCPA"), antidumping and countervailing duty remedies, and 337 investigations before the U.S. International Trade Commission ("USITC"). Nazak Nikakhtar, a partner in the firm, is co-chair of the firm's National Security practice and co-chair of the firm's CFIUS practice, representing clients in complex matters pertaining to export control and sanctions, foreign direct investment, antidumping and countervailing duty proceedings, supply chain and economic competition, and World Trade Organization dispute settlement; she previously served as Assistant Secretary and acting Under Secretary at the U.S. Department of Commerce. Resident in the firm's office in Washington, D.C., the authors may be contacted at lscheetz@wiley.law, jshane@wiley.law, and nnikakhtar@wiley.law, respectively. Nicole Hager, a law clerk at the firm, contributed to the preparation of this article.

[1] https://www.govinfo.gov/content/pkg/FR-2021-10-21/pdf/2021-22774.pdf.

[2] https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them#:~:text=Between%202019%20and%202020%2C%20ransomware,its%20annual%20Internet%20Crime%20Report.

[3] *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28,853 (Dep't Commerce May 20, 2015) (proposed rule, with request for comments).

and the cybersecurity community. The interim rule goes into effect on January 19, 2022.

BACKGROUND

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement") is a multilateral export control regime in which 42 participating countries, including the United States, agree to maintain controls on exports of certain sensitive dual-use (i.e., military and civilian uses) goods and technologies and certain munitions items.

In 2013, the Wassenaar Arrangement added specific cybersecurity items for control, as well as a definition for "intrusion software," to its list of items that should be subject to export controls in member countries.

In May 2015, BIS published a proposed rule[4] describing how it would implement these controls in the Export Administration Regulations ("EAR") and requested public comments. After hearing from the private sector, Congress and academia of potential unintended, adverse consequences of the rule on cybersecurity research and incident response, including on defensive capabilities, the United States returned to the negotiating table.

In response, in 2017, the Wassenaar Arrangement published several changes to the initial controls, and this interim rule seeks to implement those modified controls.

SCOPE OF THE NEW CONTROLS

The new rule differs from the 2015 proposal in several ways that aim to limit its scope. Specifically, it does not seek to control certain technology exchanged for vulnerability disclosure or cyber incident response, it adds "command and control" language to better target tools that can be used maliciously, and it also excludes from control certain products designed and limited to providing basic software updates and upgrades. Provided below is a brief summary of the new cybersecurity item controls:

- *New ECCNs Related to "Intrusion Software"* – The interim rule creates three new ECCNs related to the generation, command and control, or delivery of "intrusion software" – 4A005 (systems, equipment and components), 4D004 (software) and 4E001.c (technology).
    - The EAR defines "intrusion software" as software specially designed or modified to avoid detection by monitoring tools or to defeat protective countermeasures, of a computer or network-capable device by either extracting or modifying data or information on a computer or modifying the standard execution path of a program or process to execute external instructions.

[4] https://www.govinfo.gov/content/pkg/FR-2015-05-20/pdf/2015-11642.pdf.

- The software controls in ECCN 4D004 will not control software specially designed and limited to providing updates or upgrades, provided that the updates or upgrades operate only with the authorization of the system owner/administrator and that, once the update/upgrade is complete, the underlying software does not qualify as intrusion software or software meeting the criteria of ECCN 4D004.

- Additionally, to address prior concerns raised by industry and the cybersecurity community, the related technology controls expressly do not apply to "vulnerability disclosure" or "cyber incident response." "Vulnerability disclosure" is defined as "the process of identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability." "Cyber incident response" is defined as "the process of exchanging necessary information on a cybersecurity incident with individuals or organizations responsible for conducting or coordinating remediation to address the cybersecurity incident."

- *New ECCN for "IP network communications surveillance systems or equipment"* – The interim rule creates a new ECCN 5A001.j for IP network communications surveillance systems and equipment and specially designed components that perform, on a national grade IP backbone, analysis at the application layer, extraction of selected metadata and application content (e.g., voice, video, messages, attachments) and indexing of extracted data; and are specially designed to execute searches based on hard selectors and map relational networks of an individual or group of people. This new control will not apply to systems or equipment specially designed for marketing purposes, network quality of service, or quality of experience.

- *Corresponding/related changes* – BIS also made other corresponding and related changes, including adding notes to the regulations to assist exporters in determining the correct classification of their cyber products. To the extent an end item or executable software meeting the description of a cybersecurity item also includes controlled encryption or information security functionality, these latter controls in Category 5, Part 2 of the EAR's Commerce Control List ("CCL") will prevail. Similarly, if a product is controlled for Surreptitious Listening ("SL") reasons – one of the most restrictive controls on the CCL – then the SL control will trump both the cyber and encryption controls.

NEW LICENSE EXCEPTION ACE

Although the newly-added cybersecurity items will be subject to stringent National Security ("NS") export licensing requirements, the interim rule provides a broad license exception that is aimed at avoiding impediments to legitimate cybersecurity research

and incident response activities. With the exception of sanctioned countries/regions (i.e., destinations listed in Country Groups E:1 and E:2), the license exception allows for the export, reexport and transfer of cybersecurity items to most destinations without the need to apply for a specific license from BIS. However, it includes two types of end user restrictions as well as one end use restriction, as described below:

- *Government End User Restriction* – License Exception ACE includes restrictions for government end users in any country listed in Country Group D:1, D:2, D:3, D:4, or D:5 in the EAR. However, the government end user restriction does not apply to exports to Cyprus, Israel and Taiwan of (1) digital artifacts (i.e., software or technology found on an information system and showing activity pertaining to the use or compromise of, or other effects on, that information system) related to a cybersecurity incident involving information systems owned or operated by a "favorable treatment cybersecurity end user" or to a police or judicial bodies for the purposes of criminal or civil investigations of such cybersecurity incidents, or (2) cybersecurity items provided to national computer security incident response teams for the purposes of responding to cybersecurity incidents, vulnerability disclosures, or criminal investigation or prosecution of cybersecurity incidents.

  Note that a "favorable treatment cybersecurity end user" includes: (1) U.S. subsidiaries; (2) banks or other financial service providers; (3) insurance companies; and (4) civil health and medical institutions.

- *Non-Government End User Restriction* – The new license exception also includes an end user restriction applicable to non-government end users located in a country listed in Country Group D:1 or D:5, including China and Russia. However, this restriction does not apply to cybersecurity items provided to any "favorable treatment cybersecurity end user" or to vulnerability disclosure or cyber incident response. Nor does this restriction extend to "deemed exports," i.e., disclosures of controlled technology or source code to a foreign national of a D:1 or D:5 country that occur in the United States.

- *End Use Restriction* – The license exception also will not apply if the exporter knows or has reason to know that the cybersecurity item will be used to affect the confidentiality, integrity, or availability of information or information systems, without authorization by the owner, operator, or administrator of the system (including the information and processes within such systems).

WHAT THIS MEANS FOR INDUSTRY

The interim rule is more targeted and precise in its controls than the original proposal. It seeks to strike a balance between aligning with our allies to ensure that hacking tools are not used for malicious purposes, while also encouraging defensive cybersecurity activities.

Nonetheless, industry members are encouraged to carefully review the new rule and definitions and how they impact business operations. To the extent the new controls stymie or even cripple critical innovation, research and other activities of the U.S. cybersecurity industry, future engagement with BIS may be warranted.

Significant Impact on Personal Data Transfers Due to the New Standard Contractual Clauses and Final Guidance on Supplementary Measures

By Natasha G. Kohne, Michelle A. Reed, Jenny Arlington, Rachel Claire Kurzweil, Jay Jamooji and Sahar Abas*

The authors set out the key features of the updated standard contractual clauses for controllers and processors and the European Data Protection Board's finalized recommendations on the use of supplementary measures.

On September 27, 2021, all new contracts that involve cross-border personal data transfers had to incorporate the updated standard contractual clauses ("New SCCs")[1] for controllers and processors. On June 4, 2021, the European Commission adopted its highly anticipated decision on the New SCCs. These New SCCs impose more onerous obligations on importers and exporters of personal data from the European Economic Area ("EEA") and take account of Schrems II,[2] including a requirement that businesses assess the laws and practices of the destination country to determine if they would prevent them from complying with their obligations under the New SCCs. Businesses with cross-border personal data transfers out of the EEA should begin reviewing their existing contractual arrangements and data processing operations now, because the transition period is short, by December 27, 2022, all existing contracts need to be updated, and as of September 27, 2021, for new contracts the New SCCs must be used.

Supplementary measures will be an important consideration for any company relying on the New SCCs, binding corporate rules or any of the other safeguards listed in Article 46(2) of the General Data Protection Regulation ("GDPR") for data transfers to countries that do not offer sufficient data protection.

This article sets out the key features of the New SCCs and the European Data Protection Board's finalized recommendations on the use of supplementary measures.

---

* Natasha G. Kohne and Michelle A. Reed, partners in Akin Gump Strauss Hauer & Feld LLP, co-head the firm's cybersecurity, privacy and data protection practice. Jenny Arlington is counsel and Rachel Claire Kurzweil, Jay Jamooji and Sahar Abas are associates at the firm. The authors may be contacted at nkohne@akingump.com, mreed@akingump.com, jarlington@akingump.com, rkurzweil@akingump.com, jay.jamooji@akingump.com, and sahar.abas@akingump.com, respectively.

[1] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

[2] https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9793916.

KEY HIGHLIGHTS OF THE NEW SCCS

The New SCCs replace the standard contractual clauses implemented under the old Data Protection Directive ("Old SCCs"), which were last updated in 2004 and 2010 for controller-to-controller and controller-to-processor transfers, respectively.

In terms of timing, until September 27, 2021, contracts were able to be concluded on the basis of the Old SCCs. As of September 27, 2021, any new contracts relying on standard contractual clauses as the mechanism for transfer of personal data must now implement the New SCCs. Any contracts concluded on the basis of the Old SCCs may only be relied upon until December 27, 2022, and businesses will have to have transitioned to the New SCCs by that date.

The New SCCs span over 25 pages and adopt a layered, modular approach. The key highlights include the following:

1. *GDPR Spirit.* The New SCCs impose obligations on the data exporter and the data importer that are consistent with the GDPR, and the New SCCs should be read and interpreted in light of the GDPR. The New SCCs also address certain inconsistencies with the GDPR that were present in the draft proposal. For example, the obligation to notify data subjects and the relevant supervisory authority in case of a personal data breach has been updated to refer to a breach that is likely to result in a risk to the rights and freedoms of individuals, as opposed to resulting in a "significant adverse effect" which was proposed in the November 2020 drafts.

2. *Wider Range of Parties/Relationships Allowed Under a "Modular" Approach.* Under the New SCCs it is possible for more than two parties to adhere to the same set of SCCs, and additional controllers and processors (such as in the case of onward transfers of data) are permitted to accede to the SCCs throughout the life cycle of the contact by virtue of a "docking clause."

   Further, the New SCCs combine certain general clauses with a "modular approach" where parties can tailor the clauses for their specific transfer scenario, reflecting the complexity of modern processing chains.

3. *Obligation on All Parties to Conduct and Record a Transfer Impact Assessment.* The New SCCs address the concerns aired in Schrems II in relation to cross-border transfers to countries where no adequacy decision has been adopted by the European Commission.

   Specifically, the New SCCs include a declaration by the parties, in all modules, that they warrant that "they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under [the New SCCs]." The

parties are obliged to take account of certain elements in order to carry out the assessment which underpins that warranty, such as the specific circumstances of data transfers (including the content and duration of the contract, the type of recipient and purpose of processing), the laws and practices of the third country destination that are relevant to the data transfer and any safeguards in place to supplement the measures under the New SCCs. Where the parties need to introduce qualifications to that warranty, they would need to implement so-called "supplementary measures" (see below). The New SCCs also state that the parties have to document the transfer impact assessment, and make it available to the relevant data protection regulator on request.

4. *Obligations on the Data Importer to Notify Exporter of Public Authority Access Request, and Review the Legality of Such Access Request.* A data importer who receives a legally binding request from a public authority to disclose personal data transferred pursuant to the New SCCs, or who becomes aware of direct access to such data by the public authorities, is obliged to promptly notify the data exporter and, where possible, affected data subjects. If a data importer is prohibited, under the laws of the destination country, from notifying the data exporter or data subjects, the data importer must use its best efforts to obtain a waiver of the prohibition, with a view to be able to communicate as much information as possible and as soon as possible. The data importer must document its efforts and present that to the data exporter on request. To the extent permissible, the data importer must regularly provide information about the requests it receives.

   Further, the data importer must review the legality of the request for disclosure, and challenge it (including on appeal) if there are reasonable grounds to do so under the laws of the destination country or international law. When responding to a request for disclosure, the data importer has to provide the minimum amount of information possible. With yet another obligation to document, the data importer is required to document its assessment and challenge of the access request and make the documentation available to the exporter and the relevant data protection authority on request.

5. *Transparency Obligations.* The transparency obligations of a data importer who is a controller are strengthened, with the importer having to inform individuals, either directly or through the data exporter, of various details about the transfer, including "meaningful information" of the recipients in case of onward transfers of the data.

6. *Onward Transfers.* The New SCCs elaborate on the restrictions on onward transfers, stating that a data importer cannot disclose the personal data to any third party that is in the country of the data importer or in another country outside the EEA, unless certain limited exemptions apply.

7. *Strengthening the Data Subjects' Rights.* The New SCCs allow data subjects to enforce certain of their rights as third party beneficiaries against either the data importer or the data exporter. This contrasts with the position under the Old SCCs where a data subject was only permitted to proceed directly against a data importer if the data exporter, on the data subject's request, failed to take appropriate action against the data importer itself.

8. *Warranty by the Data Exporter and Obligation to Inform of the Data Importer.* The data importer has a number of obligations under the New SCCs, including those mentioned above. The New SCCs include a warranty by the data exporter that it has used reasonable efforts to determine that the data importer is able to satisfy its obligations under the New SCCs. Conversely, in the event that a data importer has reason to believe it cannot comply with the SCCs, it has to inform the data exporter.

   The data exporter must subsequently identify measures to address the situation, including in consultation with the relevant data protection authority if necessary and, in the event that no appropriate safeguards can be ensured, or if so instructed by the competent supervisory authority, the data transfer must be suspended.

9. *Submission of the Data Importer to a Regulator in the EU.* The New SCCs state that the data importer agrees to submit itself to the jurisdiction of, and cooperate with, the relevant data protection regulator of an EU member state, including by responding to enquiries, making itself available for audits and complying with any measures adopted by the regulator (such as remedial and compensatory measures).

10. *Technical and Organizational Measures.* The New SCCs envisage that the parties in all modules agree on technical and organizational measures, including to ensure the security of the data. Annex II to the New SCCs lists 17 examples of such measures which parties could adopt, including pseudonymization and encryption, protection of data during transmission and during storage, ensuring physical security of locations, ability to restore availability and access, events logging, ensuring accountability, data minimization, etc. These technical and organizational measures are envisaged regardless of whether parties implement supplementary measures or not; further, enhanced technical, organizational or contractual measures would be necessary if supplementary measures are required.

SUPPLEMENTARY MEASURES

Once parties carry out the transfer impact assessment envisaged under the New SCCs, they may decide that supplementary measures are required. Whilst such supplementary measures were referred to by the Court of Justice of the European Union ("CJEU") in its Schrems II judgment, on June 18, 2021, the European Data Protection Board

("EDPB") adopted Recommendations 01/2020[3] explaining what these measures might contain (the "Recommendations").

These measures were first published in draft form in November 2020. The CJEU had acknowledged that data exporters are responsible for verifying on a case-by-case basis if the law or practice of the third country infringes on the effectiveness of the appropriate safeguards set out in the Article 46 GDPR transfer mechanisms, or tools. In these instances, the CJEU left open the possibility of implementing supplementary measures to fill any gaps and enhance the level of protection to the level required under EU law. As the CJEU did not further specify the nature or substance of such measures, the EDPB adopted the Recommendations to provide data exporters with a series of steps to follow, potential sources of information and certain practical examples of supplementary measures that could be adopted.

Although the Recommendations are not legally binding, they serve as helpful guidance and an insight into the EDPB's approach to data transfers. The Recommendations should be closely considered by organizations relying on the New SCCs, binding corporate rules or other appropriate safeguards set out in Article 46 of the GDPR to transfer personal data outside the EEA.

Key features of the Recommendations include the following:

1. *A "Roadmap" of Steps to Determine If Supplementary Measures Are Required.* The Recommendations contain a "roadmap" of steps to take in order for data exporters to determine if supplementary measures are required to be implemented to legally transfer data outside the EEA. Broadly, the EDPB advises exporters to:

   (i) Understand their data transfers;

   (ii) Verify the transfer tools relied upon;

   (iii) Assess whether the law or practice in the third country impinges on the effectiveness of the relevant transfer tools (including standard contractual clauses, binding corporate rules and certification mechanisms); and

   (iv) If applicable, identify and adopt supplementary measures (including taking formal procedural steps and re-evaluating the level of protection at regular intervals) necessary to bring the level of protection of the data transferred to the EU standard.

2. *Access to Data by Public Authorities Must Be Considered.* In assessing whether there is anything in the law or practices in force in the third country that

[3] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

may impinge on the effectiveness of the appropriate safeguards relied upon, the Recommendations note that factors concerning access to data by public authorities "must" be considered; this includes whether public authorities may access data without the data importer's knowledge or access data through telecommunication providers.

3. *The Practices of Third Countries Must Be Considered.* Ultimately, the EDPB notes that the characteristics of each transfer must be considered, though the scope of the assessment should be limited to the legislation and practices relevant to the protection of the specific data being transferred. In particular, the Recommendations emphasize the need to consider the practices of the third country as well as the relevant legislation.

   For example, the Recommendations provide that while relevant legislation in the third country may formally meet EU standards on fundamental rights and freedoms, the practices of its public authorities may indicate they do not comply with the legislation governing their activities – in such instances, the practices of the public authorities must be taken into consideration such that the additional supplementary measures may be required. Organizations are further encouraged to take into account both their own experience and the experiences of other actors in the same sector dealing with similar data transfers.

   Likewise, the Recommendations recognize that in the absence of legislation in a third country (such as legislation on access to personal data held by the private sector) organizations cannot automatically presume the transfer tools can be effectively applied; instead, in such instances, organizations must review the indications of practices in force in the country and thereafter determine if additional supplementary measures are required.

4. *Differences Between the Recommendations and the November 2020 draft Recommendations.* Although the Recommendations broadly reflect the draft recommendations published in November 2020, there are notable differences. For example, where a transfer impact assessment indicates that the applicable legislation in the third country may be "problematic" (such as legislation not respecting the essence of the fundamental rights and freedoms recognized by the EU Charter of Fundamental Rights), the exporter may proceed with the transfer of data in the absence of additional supplementary measures, provided that the exporter considers that the problematic legislation will not be applied in practice.

   However, exporters must nevertheless be able to document and demonstrate in a detailed report that the relevant legislation will not be applied in practice. Annex 3 of the Recommendations include a comprehensive list of "possible sources" of information by which to assess a third country, such as caselaw of the CJEU and resolutions and reports from intergovernmental organizations.

Unlike the draft recommendations, the Recommendations do not limit the use of Article 49 GDPR derogations to "occasional and non-repetitive transfers," but instead emphasize that derogations cannot become "the rule" in practice and must be restricted to specific situations. The Recommendations also state that an essentially equivalent level of protection to that guaranteed within the EU must accompany personal data both "during and after the transfer."

5. *Examples of Technical, Contractual and Organizational Measures.* Annex 2 of the Recommendations set out a non-exhaustive list of possible technical, contractual and organizational measures that may be considered effective. The EDPB acknowledges that future technological, legal and organizational developments may result in the emergency of additional supplementary measures for organizations to consider. The adoption of one or more of the measures does not, however, necessarily mean that the transfer of data ensures an essentially equivalent level of protection to that which is required under EU law.

   Any supplementary measures adopted may only be deemed effective if, and only to the extent that, the measures adopted specifically address the deficiencies identified in the assessment of the third country. In the event that an essentially equivalent level of protection cannot be afforded, even with the adoption of certain supplementary measure, exporters must not transfer the personal data, unless one of the limited derogations in the GDPR can be relied upon.

6. *"Use Case" Examples.* Annex 2 contains seven "use cases," comprising practical situations in which effective measures are and are not identified. One such use case concerns a situation in which a data exporter pseudonymizes data it holds and transfer this data to a third country for analysis (e.g., for research). According to the EDPB, the pseudonymization may be deemed an effective supplementary measure if certain features are present, including: the data no longer being attributable to a specific data subject, the additional information being held exclusively by the data exporter and kept separately in a member state or third country, disclosure or unauthorized use of the additional information being prevented by technical and organizational safeguards, and the controller establishing that the pseudonymized data cannot be attributed to an identified or identifiable natural person (even if cross-referenced with such additional information) following a "thorough analysis of the data in question."

   The internal policies and procedures of an organization can be an effective supplementary measure, particularly when complimenting technical and contractual measures. One example from the Recommendations is the commitment to transparency by thorough documentation of all requests for access from public authorities.

7. *Practical Steps – Mapping International Data Transfers.* Organizations should immediately begin mapping their international data transfers, with each

transfer tied to an appropriate transfer tool. A thorough analysis will be required to identify the right supplementary measure for the specific circumstances.

ARTICLE 28 CLAUSES WHERE THERE IS NO TRANSFER OUTSIDE THE EEA

Where the processing involves a cross-border element outside the EEA, entering into the New SCCs will also satisfy the requirements of Article 28 of the GDPR, which requires that a data processing agreement, covering specific topics, is in place between a controller and a processor.

Where the processing of personal data does not involve a transfer out of the EEA, there still needs to be an Article 28 compliant agreement between a controller and a processor. On June 4, 2021, the European Commission adopted its decision on Article 28 standard contractual clauses between controllers and processors ("Article 28 Clauses").[4] The Article 28 Clauses include provisions that a data controller can impose upon a data processor to satisfy the requirements set out under Article 28 of the GDPR.

NEXT STEPS

The New SCCs significantly increase the level of diligence required both by the data importer and the data exporter before a personal data transfer can be carried out in reliance on the SCCs. Specifically, business will have to assess the impact of local laws and practices on data transfers and on the business' ability to comply with the mandatory obligations under the New SCCs. Similar to the Old SCCs, the provisions of the New SCCs are non-negotiable and non-amendable.

Businesses should begin to identify any contractual arrangements with third parties that rely on the Old SCCs for the transfer of personal data, as it will only be possible to do so until December 27, 2022. It is important to start this process in a timely manner, given that the parties will be required (among other things) to carry out local laws and practices assessments and include detailed security measures when transitioning to the New SCCs. Businesses may wish to consider whether they are best placed to make such assessments or whether obtaining local law advice would be advisable. Practices and procedures would have to be put in place in order to allow compliance with the obligations set out in the New SCCs. Changes to operations may also be required, if the transfer cannot be executed in reliance on the New SCCs.

Businesses that are entering into new contracts with third parties must now adopt the New SCCs at the outset, as it is no longer permitted to enter into new contracts using the Old SCCs.

---

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0915&locale-en.

Australian Privacy Overhaul on the Horizon

By Sophie Dawson and Emma Croft*

In this article, the authors discuss a proposed privacy code that, if implemented, would have a fundamental impact on the reach, enforcement risk and effect of Australian privacy laws.

In Australia, extensive privacy reforms have now been canvassed in more detail than previously, and a bill proposing a privacy code for certain online businesses has been released. If implemented, these changes will have a fundamental impact on the reach, enforcement risk and effect of Australian privacy laws. It is important for entities that carry on business in Australia to consider the proposed changes carefully so that any unacceptable practical implications can be addressed before the laws are finalized and implemented. Submissions will be accepted until January 10, 2022.

COMPREHENSIVE UPDATE

On October 25, 2021, the Attorney General released an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the "Online Privacy Bill") (setting out some interim reforms). Immediate changes include broadening the scope of the Privacy Act to cover further practices of overseas entities operating in Australia, an online privacy code for social media and platforms and certain others, together with penalties of up to potentially AU$10,000,000 or more for some companies. The exposure draft of the Online Privacy Bill was released in tandem with an extensive discussion paper published as part of a broader review of the Privacy Act, which seeks submissions on further reform proposals by January 10, 2022.[1]

ONLINE PRIVACY BILL REFORMS

The Online Privacy Bill addresses four broad categories of reform:

- The Online Privacy ("OP") code;
- Enforcement of the Privacy Act;

* Sophie Dawson, a partner in the Sydney, Australia, office of Bird & Bird, is head of the firm's Dispute Resolution practice in Australia. She specializes in media and technology advice and disputes. Emma Croft is an associate in the firm's Dispute Resolution Group in Sydney. The authors may be contacted at sophie.dawson@twobirds.com and emma.croft@twobirds.com, respectively.

[1] The exposure draft Online Privacy Bill and the discussion paper released by the Attorney General can be viewed at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/.

- Office of the Australian Information Commissioner ("OAIC") information-sharing powers; and
- Amendments to the extraterritorial provisions.

Each of these categories is described in further detail below.

OP CODE

Development of an OP Code is a key reform sought to be implemented by the Online Privacy Bill. As with the Australian Privacy Principles ("APPs") and Credit Reporting ("CR") Codes able to be developed under the Privacy Act, the OP Code is to be developed by the relevant industry, although the OAIC will have the discretion to develop the OP code itself in certain circumstances, for example where no suitable OP Code developer could be found. After the Online Privacy Bill receives royal assent, the OP Code will need to be developed and registered within 12 months.

The OP code is set to apply to the following categories of private sector organizations ("OP organizations"):

1. Organizations that provide social media services;
2. Organizations that provide data brokerage services; and
3. Large online platforms (being those organizations not falling within the above two categories that collect personal information about an individual in the course of or in connection with providing access to information, goods or services by use of an electronic service and that have had over 2,500,000 end-users in Australia in the past year). This does not include customer loyalty schemes, which are being separately considered as part of the broader Privacy Act review.

OP organizations will need to meet the requirements of the OP code, as well as the ordinary provisions of the Privacy Act. The OP code requirements are set to include the following:

- Entities must ensure that their privacy policy clearly and simply explains the purposes for which they collect, hold, use and disclose personal information;
- All notices provided, including those issued in accordance with APP 5, must be clear and understandable, current and provided in a timely manner;
- Organizations must ensure that, when they seek consent from individuals, the consent is voluntary, informed, unambiguous, specific and current. In respect of sensitive information, organizations will also need to seek renewed consent periodically or when circumstances change;

- Organizations must take reasonable steps to not use or disclose, or to not further use or disclose, an individual's personal information upon request from that individual; and

- Elevated protections will apply for children and vulnerable groups. For example, social media organizations will be required to take all reasonable steps to verify the age of individuals who use the service, to only collect, use and disclosure of personal information is fair and reasonable and must obtain parental or guardian consents for those under the age of 16.

The OP code may also provide for the following:

- How one or more of the APPs are to be applied or complied with by the OP organizations;

- Additional (but not contrary or inconsistent) requirements to the APPs;

- Mechanisms to deal with the internal handling of complaints; and/or

- The reporting of complaints or number of end-users in Australia to the OAIC.

The OAIC will have the power to investigate potential breaches of the OP code, either following a complaint or on its own initiative. If the OAIC finds that a breach has occurred, its full range of enforcement powers, including those set out below, will be available to it.

PRIVACY ACT ENFORCEMENT

Section 13G of the Privacy Act prohibits entities from committing serious or repeated interferences with the privacy of an individual. The Online Privacy Bill seeks to increase the penalty applicable for a contravention of this section by a body corporate from AU$2.22 million to the greater of the following:

- AU$10,000,000;

- If able to be determined, three times the value of the benefit that the body corporate (and, if applicable its related body corporate) obtained from the conduct constituting the contravention; or

- If the court cannot determine the value of that benefit derived from the conduct, 10 percent of the body annual corporate's turnover from the year before the conduct commenced.

In addition to increasing the applicable maximum penalty for interferences with privacy, the Online Privacy Bill also seeks to strengthen the OAIC's enforcement powers as follows:

- Introducing a new infringement notice provision for failing to give information or providing a document or record when required to do so as part of an investigation (with associated additional civil penalty provisions);
- Creating a new criminal penalty for multiple instances of non-compliance with the above requirements;
- Expanding the types of declarations the OAIC can make in a determination following an investigation; and
- Enhancing the OAIC's capacity to conduct assessments.

OAIC INFORMATION-SHARING POWERS

The Online Privacy Bill also seeks to provide the OAIC with the ability to share information or documents it acquires in the course of exercising its powers with law enforcement bodies, alternative complaint bodies (defined to include: the Australian Human Rights Commission, the Ombudsman, the Postal Industry Ombudsman, the Australian Public Service Commissioner, the Inspector General of Intelligence and Security, the eSafety Commissioner or another recognized external dispute resolution scheme) and state, territory or foreign privacy regulators. However, this is only permitted where the OAIC is satisfied that the receiving authority has satisfactory arrangements in place for maintaining the security of the information or documents provided. This may be particularly significant for organizations who are subject to data breaches or other privacy-related incidents in multiple jurisdictions.

The OAIC will also be permitted to disclose such information or documents (including, in certain circumstances, those obtained through use of the notifiable data breach scheme) where it is satisfied that it is in the public interest to do so.

EXTRATERRITORIAL PROVISIONS

Currently the extraterritorial application of the Privacy Act only extends to organizations not incorporated in Australia that carry on business in Australia where the personal information "was collected or held" by the organization "in Australia or an external Territory, either before or at the time of the act or practice."

The Online Privacy Bill seeks to remove the condition that the relevant personal information be held or collected from sources inside of Australia. This will have the effect of requiring foreign organizations who carry on a business in Australia to meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia.

DISCUSSION PAPER

The discussion paper released by the Attorney General sets out a wider tranche of ideas and proposals, ahead of the release of the Privacy Review's Final Report to be considered by the government. This includes:

- Broadening the definition of personal information, for example to include technical information and inferred information;
- Removal/modification of the employee records exemption;
- Modification of the journalism exception, for example by introducing a public interest requirement into the journalism exemption;
- Amendment of the matters required to be included as part of an organization's privacy policy (in respect of direct marketing);
- Amendment of the matters required to be notified as part of a collection notice issued under APP 5.2;
- Additional requirements for information handling, notices and consent in respect of the personal information of children;
- An additional requirement in respect of collection, use and disclosure of personal information, namely that it be fair and reasonable in the circumstances;
- An additional requirement that risk-mitigation steps be taken in respect of particular privacy risks in respect of direct marketing;
- New requirements for pro-privacy default settings on websites, for example requiring opt-in as opposed to opt-out;
- Changed rules for cross-border flows of data;
- Introduction of penalties for re-identification of de-identified information released by Commonwealth agencies;
- Replacement of the "de-identification" requirements with the higher standard of anonymization;
- Additional requirements for mandatory notification following a eligible data breach occurring; and
- Increased individual rights, such as a right of erasure, a direct right of action and a tort of privacy.

The Attorney General's department is accepting submissions on the above until January 10, 2022.

OTHER ONGOING REVIEWS

Separately, the federal Australian government is currently conducting reviews into:

- Regulation of adtech practices;
- Cybersecurity regulation, for example by way of minimum standards;
- Online harm and digital platforms generally; and
- Security incidents affecting critical infrastructure (which will be broadened to include sectors such as the communications and data storage or processing sectors).