IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

TWITTER, INC.,	)	
	)	
Plaintiff and Counterclaim-Defendant,	)	
	)	
v.	)	C.A. No. 2022-0613-KSJM
	)	
ELON R. MUSK, X HOLDINGS I, INC., and X HOLDINGS II, INC.,	)	
	)	
Defendants and Counterclaim-Plaintiffs.	)	

MEMORANDUM OPINION

Date Submitted: September 6, 2022
Date Decided: September 13, 2022

Peter J. Walsh, Jr., Kevin R. Shannon, Christopher N. Kelly, Mathew A. Golden, Callan R. Jackson, POTTER ANDERSON & CORROON LLP, Wilmington, Delaware; Brad D. Sorrels, WILSON SONSINI GOODRICH & ROSATI, P.C., Wilmington, Delaware; William Savitt, Bradley R. Wilson, Sarah K. Eddy, Ryan A. McLeod, Anitha Reddy, Noah B. Yavitz, WACHTELL, LIPTON, ROSEN & KATZ, New York, New York; *Counsel for Plaintiff and Counterclaim-Defendant Twitter, Inc.*

Edward B. Micheletti, Lauren N. Rosenello, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP, Wilmington, Delaware; Alex Spiro, Andrew J. Rossman, Christopher D. Kercher, Silpa Maruri, QUINN EMANUEL URQUHART & SULLIVAN LLP, New York, New York; *Counsel for Defendants and Counterclaim-Plaintiffs Elon R. Musk, X Holdings I, Inc., and X Holdings II, Inc.*

McCORMICK, C.

This is an action for specific performance of an April 25, 2022 merger agreement under which Elon R. Musk and two entities he owns, X Holdings I, Inc. and X Holdings II, Inc. (with Musk, "Defendants"), agreed to acquire Twitter, Inc. To communicate about the Twitter transaction, Musk used two sets of email accounts: one sponsored by Space Exploration Technology Corp. ("SpaceX") and the other by Tesla, Inc. Musk asserted attorney-client privilege over emails in the SpaceX and Tesla accounts and withheld them in discovery. Twitter has moved to compel those documents.

To support a claim of attorney-client privilege, Musk must demonstrate that he had an objectively reasonable expectation of confidentiality in the SpaceX and Tesla emails. In certain circumstances, this court had applied the four-factor analysis of *In re Asia Global Crossing, Ltd.*[1] to determine whether an employee had an objectively reasonable expectation of privacy in personal communications in their work emails. The *Asia Global* analysis looks to whether company policies or practices reduce an employee's expectation of privacy in the employee's work emails.[2] SpaceX and Tesla email policies make clear that employees have no privacy interest in their work emails and warn that the companies reserve the right to monitor those emails. Citing to the plain language of those policies, Twitter argues that Musk had no reasonable expectation of privacy in his SpaceX and Tesla emails.

---

[1] *In re Inform. Mgmt. Servs., Inc. Deriv. Litig.*, 81 A.3d 278, 286–87 (Del. Ch. 2013) ("*IMS*") (applying *Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)).

[2] *IMS*, 81 A.3d at 286.

Although Twitter's argument is a compelling one in many ways, Musk nevertheless prevails on this motion. To support his claim of attorney-client privilege, Defendants submitted affidavits from Musk, IT managers from SpaceX and Tesla, and the head of Tesla's legal department.[3] Those affidavits state that each company had a policy of limiting the circumstances in which they would monitor employee emails. They further state, unequivocally, that Musk had "unrestricted" personal use of his Tesla email account, that "no one" at Tesla can access those emails without Musk's consent or "to the extent legally necessary," and that "nobody" at SpaceX can access his email account without Musk's express consent.[4] These additional facts make Musk's expectation of privacy objectively reasonable. Twitter's motion is denied.

I. FACTUAL BACKGROUND

Musk is CEO of both SpaceX and Tesla,[5] but SpaceX and Tesla are third parties with no involvement in the Twitter transaction.

Both SpaceX and Tesla have internal policies that bear on employees' expectation of privacy in information found in company-sponsored email accounts.

[3] C.A. No. 2022-0613-KSJM, Docket ("Dkt.") 394, Aff. of Elon R. Musk ("Musk Aff."); Dkt. 395, Aff. of SpaceX Manager of Executive IT Support Alex Stillings ("Stillings Aff."); Dkt. 397, Aff. of Twitter Staff Technical Investigator and Digital Forensics Mgr. John Shumway ("Shumway Aff."); Dkt. 396, Aff. of Senior Commercial Counsel Dinna Eskin ("Eskin Aff.").

[4] Shumway Aff. ¶¶ 10, 14; Stillings Aff. ¶ 15; Eskin Aff. ¶¶ 6–8.

[5] Musk Aff. ¶¶ 1–2.

SpaceX permits its employees to use their SpaceX email accounts for communications unrelated to their SpaceX work, subject to certain guidelines and monitoring.[6]

As to "Email and Internet," the SpaceX Employee Handbook provides that:

> SpaceX allows email/Internet communications and cell phone usage unrelated to work. However, such communications must be kept to a minimum, cannot interfere with work performance or business needs, cannot breach any other Company policy (such as SpaceX's policy against harassment), and must comply with the guidelines discussed in this section.
>
> Company computers, cell phones, tablets, laptops and other electronic devices provided or paid for by SpaceX are owned by SpaceX. The Company reserves the right to review all emails, text messages and other communications that are sent or received on SpaceX equipment, SpaceX accounts, or the SpaceX network, and you should have no expectation of privacy or confidentiality when using these resources.
>
> . . . The rule of thumb when using the SpaceX email system and computer network is to use them judiciously because they're valuable Company resources. Please see Computer Acceptable Use Policy for more info.[7]

SpaceX's Computer Acceptable Use Policy provides that:

> [N]etwork accounts providing electronic mail . . . are property of SpaceX. These systems are to be used for business purposes in serving the interests of the company. . . .
>
> Employees . . . should be aware that the data they create on the corporate systems remains the property of SpaceX. The SpaceX Information Security team cannot guarantee the

[6] Stillings Aff. ¶ 8.

[7] Stillings Aff., Ex. A at SPACEX_00000035.

> confidentiality of information stored or accessed on any network device belonging to SpaceX.[8]

SpaceX's Information Security Policy similarly provides:

> Employees . . . with network access should be aware that the data they create or store on corporate systems remains the property of SpaceX. The SpaceX Information Security team cannot guarantee the privacy of information stored on any device belonging to SpaceX.[9]

The policy further provides that

> authorized individuals within SpaceX may monitor equipment, systems and network traffic at any time.[10]

Musk believed that communications on his SpaceX accounts were private and that he was authorized to use each account for personal use on an unrestricted basis.[11] Musk has stated that the above SpaceX policies do not apply to him. He averred that "SpaceX's policy and practice with respect to my communications is that nobody associated with SpaceX is permitted to access my emails without my express consent."[12] He further averred that his SpaceX email accounts "contain emails with sensitive information, including some whose disclosure could violate the State Department's International Traffic in Arms Regulations . . . and could compromise national security. The extreme sensitivity of my SpaceX Email Accounts is recognized by SpaceX's security team and leadership."[13]

---

[8] Stillings Aff., Ex. B at SPACEX_00000100.

[9] Dkt. 375 ("Pl.'s Third Disc. Mot."), Ex. E at SPACEX_00000093.

[10] Stillings Aff., Ex. B at SPACEX_00000100.

[11] Musk Aff. ¶¶ 6, 9.

[12] *Id.* ¶ 8.

[13] *Id.* ¶ 11.

To Musk's knowledge, no one at either company has accessed his email accounts except for pre-authorized purposes, such as producing emails in this litigation.[14] SpaceX's IT Manager submitted an affidavit corroborating Musk's statements.[15]

Tesla's policies permit monitoring of Tesla emails accounts and warn employees that they have no expectation of privacy over information transmitted through Tesla emails.[16]

The use of Tesla email accounts is governed by the company's Global Information Security Policy, the latest version of which was approved on March 23, 2022.[17] That policy states that it "applies to the entire Tesla organization," and "[i]t is Tesla's intent that [it] be fully implemented and followed."[18]

Section 10.2 of Tesla's Global Information Security Policy "encourage[s]" employees to use Tesla email accounts for company-related activities.[19] It provides that:

> Employees of the Company are encouraged to use electronic mail (e-mail) . . . for Company-related activities and to facilitate the efficient exchange of useful information. Access to e-mail, messaging platforms, and Company computers is a privilege and certain responsibilities accompany that privilege.
>
> By using Tesla's electronic mail, data, voicemail, messaging systems and the utilization of other communications equipment (including company computers, phones, and applications installed on personal owned devices), users knowingly and

[14] *Id.* ¶¶ 12, 18.

[15] Stillings Aff. ¶¶ 15–16.

[16] Shumway Aff., Ex. D § 10.2, at TESLA_00000009–10.

[17] *Id.* § 14 at TESLA_00000014.

[18] *Id.* § 2 at TESLA_00000003.

[19] *Id.* § 10.2, at TESLA_00000009–10.

> voluntarily consent to being monitored by Tesla, acknowledging Tesla's right to conduct such monitoring, and acknowledge that they have no expectation that said systems, communications, and equipment are private to any employee.
>
> Employees should not use Tesla owned communications systems and devices as a means of communicating or storing information about their personal lives. These systems and devices are monitored for compliance with this and other policies.
>
> Electronic and phone communications, including electronic mail . . . and the contents stored locally on computers, cloud storage, removable media and provided by Company are the sole property of Tesla.[20]

Tesla's Internet Usage Policy expressly states that employees have no expectation of privacy over their Tesla emails:

> [A]ll Tesla employees . . . and all other persons using/connected to Tesla networks ("users") must comply with the following policy whether they are using their own device or one provided by Tesla.
>
> Users have no expectation of privacy with respect to information transmitted over, received by, or stored in any Tesla device, network, server, computer, system, software platform, or other equipment or device ("Tesla devices or networks") owned, leased, or operated by or on behalf of Tesla or used by users for company purposes.[21]

Notwithstanding the above policies, a manager in Tesla's Security Intelligence Team ("SI Team"), John Shumway, submitted an affidavit stating that "Tesla has written procedures in place that limit the circumstances under which Tesla email accounts may be

---

[20] *Id*. § 10.2, at TESLA_00000009–10; *see also id.* § 9.7 (Personal Monitoring), at TESLA_00000009 ("Employees may be subject to electronic monitoring when using Tesla information systems.").

[21] Pl.'s Third Disc. Mot., Ex. C at TESLA_00000071.

accessed for employees."[22] He explained that "[a] Tesla employee's email account may not be accessed by the SI Team except as duly authorized in an investigation of potential misconduct . . . or if it was necessary to do so in order to comply with legal obligations."[23] All employee investigations require case-by-case authorization by Musk or the head of Tesla's legal department.[24] Shumway is unaware of any instance where Tesla has reviewed an employee's email based on a suspicion that it was used for purposes "unrelated to Tesla's business."[25]

Musk believed that communications on Tesla email accounts were private and that he was authorized to use each account for personal use on an unrestricted basis.[26] To his knowledge, no one at the company has accessed his email accounts except for pre-authorized purposes, such as producing emails in this litigation.[27] Shumway corroborated these statements in his affidavit and further averred that "[n]o one at Tesla can review Mr. Musk's emails without his consent except to the extent legally necessary."[28] The head of Tesla's legal department, Dinna Eskin, submitted an affidavit to the same effect, stating "that nobody in Tesla's SI Team can review emails in Mr. Musk's Tesla email accounts

[22] Shumway Aff. ¶ 4.

[23] *Id.* ¶ 5.

[24] *Id.* ¶ 6.

[25] *Id.* ¶ 9.

[26] Musk Aff. ¶¶ 13, 16.

[27] *Id.* ¶¶ 15, 18.

[28] Shumway Aff. ¶ 14.

without first obtaining permission to do so from Mr. Musk or from the General Counsel (or the person in the role equivalent to General Counsel), unless legally necessary."[29]

In this litigation, Defendants asserted attorney-client and work-product privileges over Musk's emails in his SpaceX and Tesla accounts. On September 2, 2022, Twitter moved to compel Musk's SpaceX and Tesla emails over which Musk asserted attorney-client privilege.[30] Musk opposed the motion.[31] The court heard oral argument on September 6, 2022.[32]

II. LEGAL ANALYSIS

To be eligible for the protections of the attorney-client privilege under Delaware Rule of Evidence 502, a communication must be "confidential."[33] "A communication is 'confidential' if not intended to be disclosed to third persons other than those to whom disclosure is made in furtherance of the rendition of professional legal services to the client or those reasonably necessary for the transmission of the communication."[34] Confidentiality for Rule 502 purposes has subjective and objective aspects. "A party's subjective expectation of confidentiality must be objectively reasonable under the

[29] Eskin Aff. ¶ 8.

[30] Pl.'s Third Disc. Mot.

[31] Dkt. 392 ("Defs.' Opposition").

[32] Dkt. 412.

[33] D.R.E. 502(b).

[34] D.R.E. 502(a)(2).

circumstances."[35] Whether a party had an objectively reasonable expectation of privacy is decided on a case-by-case basis;[36] it is not the sort of analysis that lends itself to "bright-line rules."[37] The party asserting privilege bears the burden of proving it.[38]

This court has applied the factors articulated in 2005 by a bankruptcy court of the Southern District of New York in *Asia Global* to determine, in certain circumstances, whether a user had an objectively reasonable expectation of privacy over personal communications in their work emails.[39] Those factors look primarily to whether company policies and historical practices made it reasonable for employees to expect privacy in company-sponsored emails.

Twitter argues under *Asia Global* that, although the policies of both SpaceX and Tesla state that email accounts are subject to monitoring and Tesla's policies expressly state that users have no expectation of privacy, Musk used his SpaceX and Tesla accounts to communicate about the Twitter transaction. Under these circumstances, Twitter contends that Musk lacked any reasonable expectation of privacy over his SpaceX and Tesla emails, and thus Musk cannot support his claim of attorney-client privilege.

---

[35] *IMS*, 81 A.3d at 285 (emphasis added) (citing *Upjohn v. United States*, 449 U.S. 383, 389, 395 (1981)).

[36] *IMS*, 81 A.3d at 286–87 (citing *Asia Global*, 322 B.R. at 257).

[37] *In re Dell Techs., Inc. Class V S'holders Litig.*, C.A. No. 2018-0816-JTL at 48:13–18 (Del. Ch. Sept. 17, 2021) (TRANSCRIPT).

[38] *In re WeWork Litig.*, 2020 WL 7624636, at *2 (Del. Ch. Dec. 22, 2020) (citing *Moyer v. Moyer*, 602 A.2d 68, 72 (Del. 1992)).

[39] *IMS*, 81 A.3d at 285–86 (citing *Asia Global*, 322 B.R. at 256–57).

Defendants advance three arguments in response. Their primary argument is that *Asia Global* should not apply where, as here, the party seeking to pierce the privilege is an outsider to the corporate entity owning the email accounts at issue.[40] In the alternative, Defendants argue that Musk has met his burden under *Asia Global*.[41] As a fallback, Defendants contend that Twitter's *Asia Global* argument does extend to work product.[42]

Although Defendants' primary argument urging a course correction in Delaware law raises interesting issues worthy of extensive discussion,[43] the press of time requires a more direct approach to resolving the parties' dispute. Defendants' second argument under *Asia Global* prevails. For that reason, this decision does not address Defendants' primary or fallback arguments.

Under *Asia Global*, four factors guide the court's analysis of whether an employee had a reasonable expectation of privacy in his work emails:

---

[40] Defs.' Opposition at 12–15.

[41] *Id*. at 15–25.

[42] *Id*. at 25–27.

[43] *Compare WeWork*, 2020 WL 7624636, at *5–6 (rejecting the argument that *Asia Global* should not apply where the party seeking to pierce the privilege is an outsider to the corporate entity owning the email accounts at issue where the proponent failed to address federal authorities on point), *with IMS*, 81 A.3d at 296–98 (cautioning, in dicta motivated in part by concerns over derivative litigation, against applying *Asia Global* where the party seeking to pierce the privilege is an outsider to the corporate entity owning the email accounts), *Dell* Tr. at 55:1–13 (applying *Asia Global* in the outsider context but noting the outsider or "stranger" status of the movant when denying the motion to compel), and *In re Appraisal of Ancestry.com*, C.A. No. 8173-VCG at 18:18–19:1 (Del. Ch. Feb. 19, 2014) (TRANSCRIPT) (tacitly rejecting the *Asia Global* framework and instead asking whether the party asserting privilege was adverse to the corporate entity owning the email accounts).

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[44]

"No one factor is dispositive,"[45] although the first factor is often viewed as the "dominant" one.[46] "Several of the . . . factors have been refined through subsequent application."[47]

The first *Asia Global* factor weighs "in favor of production when the employer has a clear policy banning or restricting person use, where the employer informs employees that they have no right of personal privacy in work email communications, or where the employer advises employees that the employer monitors or reserves the right to monitor work email communications."[48]

The court looks foremost to the language of the policies when applying the first factor. SpaceX policies do not impose an outright ban on personal use. SpaceX policies do warn that users have "no expectation of privacy or confidentiality when using [SpaceX] resources" and also "reserve[] the right to review all emails, text messages and other communications that are sent or received on SpaceX equipment, SpaceX accounts, or the SpaceX network."[49]

---

[44] *Asia Global*, 322 B.R. at 257 (internal citation omitted).

[45] *IMS*, 81 A.3d at 287 (citing *Asia Global*, 322 B.R. at 258–59).

[46] *Dell* Tr. at 55:17–20.

[47] *IMS*, 81 A.3d at 287.

[48] *Id.* at 287; *see also WeWork*, 2020 WL 7624636, at *2 (same).

[49] Stillings Aff., Ex. A at SPACEX_00000035.

Similarly, Tesla policies do not impose an outright ban on personal use, although they discourage it and instruct that "[e]mployees should not use Tesla owned communications systems and devices as a means of communicating or storing information about their personal lives."[50] Tesla policies further warn that "[u]sers have no expectation of privacy with respect to information transmitted over, received by, or stored in any Tesla device, network, server, computer, system, software platform, or other equipment or device," and advise that Tesla "systems and devices are monitored for compliance with [Tesla policies]."[51]

Although neither company expressly bans personal use of company emails, each reserves the right to monitor emails in work accounts and Tesla makes clear that users have no privacy interest in work emails.

This court has held that comparable policies weigh in favor of production under the first *Asia Global* factor. In *WeWork*, the court treated policies nearly identical to those of Tesla as weighing in favor of production and effectively dispositive of the *Asia Global* analysis.[52] In *IMS*, the court concluded that an email use policy comparable to SpaceX and less strict than Tesla weighed in favor of production under the first *Asia Global* factor. The

---

[50] Shumway Aff., Ex. D § 10.2, at TESLA_00000009–10 ("encourag[ing]" Tesla employees to use Tesla email for Tesla-related activities).

[51] Pl.'s Third Disc. Mot., Ex. C at TESLA_00000071; Shumway Aff., Ex. D § 10.2 at TESLA_00000009–10.

[52] *WeWork*, 2020 WL 7624636, at *2–3 (finding that the first *Asia Global* factor weighed in favor of production when the applicable policy did not ban personal use of email but did reserve the company's right to review emails and included "an explicit warning that employees should have no expectation of privacy when using their [workplace] email accounts").

policy in *IMS* placed employees on notice that their work emails could be monitored but stopped short of expressly warning that employees lacked any privacy right in the emails.[53]

A few mitigating considerations blunt the blow of the SpaceX and Tesla policies to Defendants' arguments. The first is that, despite the broad language by which SpaceX and Tesla reserve the rights to monitor employee emails, both companies have policies limiting the grounds for monitoring employee emails. SpaceX and Tesla access employee emails only after securing the approval of the Legal and Human Resources departments, and only where necessary to investigate an issue or conduct business (such as after an employee has left the company).[54] These policies suggest that an employee might expect privacy over personal communications unless the employee is acting contrary to company guidelines. Because the guidelines do not expressly ban personal use, one might reasonably surmise that the companies would not review personal communications of employees who are otherwise compliant with company policies. In *Dell*, the court held that a similar combination of policies, albeit coupled with the fact that the company granted the user a company email despite the user's retired status, supported a reasonable expectation of privacy over personal emails on the company server.[55] Here, although Musk is not retired,

---

[53] *IMS*, 81 A.3d at 289.

[54] *See* Stillings Aff. ¶¶ 11–14 (discussing SpaceX's general procedures that limit the circumstances under which a SpaceX email account may be accessed); Shumway Aff. ¶¶ 4–8 (discussing Tesla's written procedures that limit the circumstance under which Tesla email accounts may be accessed for employees).

[55] *Dell* Tr. at 52:16–53:12, 54:9–24.

the limitations on monitoring imposed by SpaceX and Tesla make Musk's expectation of privacy more reasonable.

As the second and perhaps most forceful mitigating consideration, Defendants argue that the "default" policies of SpaceX and Tesla do not apply to Musk, and that each company adopted "Musk-specific" rules.[56] For this, Defendants rely exclusively on the affidavits of Musk, IT managers from SpaceX and Tesla, and the head of Tesla's legal department. Those affidavits state, unequivocally, that Musk had "unrestricted" personal use of his Tesla email account, that "no one" at Tesla can access those emails without Musk's consent except "to the extent legally necessary," and that "nobody" at SpaceX can access his email account without Musk's express consent.[57]

A cynic might doubt that Musk-specific policies exist at SpaceX and Tesla. Defendants' factual arguments to that effect rely solely on the affidavits of Musk, who has a lot at stake in this litigation, and three of his direct reports, and none of the affidavits are supported by any corporate records reflecting Musk-specific rules. Still, to this jurist, the evidence rings true. The court has little doubt that neither SpaceX nor Tesla view him as on par with other employees, that he has the power to direct operational decisions, and that nobody at either company would access his information without first obtaining his

[56] Defs.' Opposition at 19–20.

[57] Musk Aff. ¶¶ 8, 13; Shumway Aff. ¶¶ 10, 14; Stillings Aff. ¶ 15; Eskin Aff. ¶¶ 6–8.

approval. One can debate whether this corporate reality makes for good "corporate hygiene,"[58] but it is difficult to discredit the recitation of the facts.[59]

Taken together, the companies' policies limiting the circumstance in which employee emails will be monitored coupled with the evidence of Musk-specific policies outweighs the generic policies that diminish employee privacy expectations. The first *Asia Global* factor weighs against production of documents.

The second *Asia Global* factor looks to the email sponsor's historical practice of monitoring employee emails in accordance with its policies. "[S]ome decisions have held that if any employer reserves the right to monitor work email, then whether it actually does so is irrelevant."[60] By contrast, this court views the second factor as probative as a standalone inquiry. "[T]he employer's actual conduct with respect to monitoring remains an appropriate factor to consider, particularly if the employer has made specific

---

[58] *Dell* Tr. at 42:23.

[59] Defendants also point to Musk's status as an executive/"employer" within the companies as supportive of his expectation of privacy, relying on a bench ruling applying *Asia Global* in *In re Shawe & Elting LLC*, C.A. No. 9700-CB (Del. Ch. Mar. 2, 2015) (TRANSCRIPT). There, Chancellor Bouchard denied a motion to compel Elizabeth Elting's spousal communications found on the Transperfect Global, Inc. server, observing that the employee handbook "was not intended to apply to Ms. Elting, who more accurately could be viewed as an employer and not one of the employees to whom the handbook was intended to govern." *Id.* at 1595:22–1496:3. Elting, however, was not solely a company executive; she also owned 50% of Transperfect's stock and was one of only two directors. *Id*. at 1597:3–5. It was her stock holdings and board representation that tilted Elting toward the "employer" side of the analysis. Here, Musk does not rely on stock ownership or board representation to support his expectation of privacy. For this reason, *Shawe* does not aid Defendants' arguments. For other reasons discussed above the line, Defendants' arguments nevertheless prevail.

[60] *IMS*, 81 A.3d at 289 (citing cases).

representations or taken specific actions inconsistent with the monitoring policy and the employee can show detrimental reliance."[61]

According to Defendants' affidavits, SpaceX and Tesla personnel have never monitored, accessed, or reviewed Musk's email except for purposes he had preauthorized or as legally necessary.[62] The "legally necessary" caveat does not undermine the force of this factual representation. Just like individuals, companies are required to comply with legal obligations. Individuals have an expectation of privacy in their home; the mere fact that a private residence could be searched with an appropriate warrant does not eliminate an individual's reasonable expectation of privacy in their home for all purposes. Similarly, employees have an expectation of privacy at work (subject to office procedures and practices); the fact that a company may need to access employee data to comply with legal obligations does not eliminate an employee's expectation of privacy for all purposes.

The second *Asia Global* factor weighs against production of documents.

The third *Asia Global* factor asks whether third parties have a right to access to the computer or emails at issue. "In a work email case, this factor largely duplicates the first and second factors, because by definition the employer has the technical ability to access the employee's work email account."[63] This factor is most helpful in inapposite scenarios, "when analyzing webmail or other electronic files that the employer has been able to

---

[61] *IMS*, 81 A.3d at 289 (citing cases); *see also WeWork*, 2020 WL 7624636, at *3 ("The second factor asks whether the company monitors the use of the employee's computer or e-mail.").

[62] Stillings Aff. ¶ 16; Shumway Aff. ¶ 11; Musk Aff. ¶¶ 12, 18.

[63] *IMS*, 81 A.3d at 290; *see also WeWork*, 2020 WL 7624636, at *4 (same).

intercept, recover, or otherwise obtain."[64] In that scenario, the court considers employee efforts to protect the information, such as encryption or deletion efforts.[65] This motion does not involve that scenario. Rather, this motion concerns documents on company-sponsored email accounts, not other documents intercepted by an employer. In this circumstance, the third factor is entirely duplicative of the first two factors.

Like the first two factors, the third *Asia Global* factor weighs against production of documents.

The fourth *Asia Global* factor considers the employee's knowledge regarding the company's policies and practices. "If the employee lacked knowledge of the email policy," then this factor weighs against production.[66] "If the employee had actual or constructive knowledge of the policy," then this factor weighs in favor of production.[67] "Decisions have readily imputed knowledge of an employer's policy to officers and senior employees."[68]

Here, it cannot be disputed that Musk had general knowledge of the SpaceX and Tesla policies and actual knowledge of the policies and practices he described as Musk-specific. Knowledge of all SpaceX and Tesla policies and practices can be "readily imputed" to Musk as well given his positions at the companies. But because the policies

[64] *IMS*, 81 A.3d at 290–91.

[65] *Id.* at 291.

[66] *Id.*

[67] *Id.* at 291–92.

[68] *Id.* at 292; *see also WeWork*, 2020 WL 7624636, at *4 (same).

and practices on balance favor Musk's position, his knowledge of those policies too weighs in his favor.

The fourth *Asia Global* factor weighs against production of documents.

III. CONCLUSION AND INSTRUCTION REGARDING PUBLIC FILINGS

Under the *Asia Global* factors, Musk has demonstrated a reasonable expectation of privacy over his SpaceX and Tesla emails. Musk has therefore proven the only element of his claim of attorney-client privilege over those emails challenged by Twitter. Twitter's motion to compel production of these documents is therefore denied.

There is another matter. I have reviewed the publicly filed version of Twitter's motion and Defendants' opposition concerning Musk's SpaceX and Tesla email accounts. The redactions were too heavy. I discussed some of the redacted information in this decision. Because the public should have access to information that speaks directly to the merits of the parties' discovery dispute,[69] I did not omit or redact that information from this decision. None of the information discussed in this decision is truly sensitive or confidential under Court of Chancery Rule 5.1 in any event. The parties are instructed to prepare new public filings, eliminating redactions as to information set forth in this

[69] *See generally Tornetta v. Musk*, 2022 WL 130864, at *3 (Del. Ch. Jan. 14, 2022) ("Court of Chancery Rule 5.1 exists to protect the public's right of access to information about judicial proceedings and makes clear that most information presented to the Court should be made available to the public. The right of access enables the public to judge the product of the courts in a given case, which in turn, helps ensure quality, honesty and respect for our legal system. With these goals in mind, the default presumption under Rule 5.1 is that proceedings in a civil action are a matter of public record." (internal quotations and footnotes omitted) (cleaned up)).

decision. Defendants are also instructed to file public versions of the four affidavits on which Defendants relied.