ISACA

消除欺騙性的隱私實務：

透過解決暗黑模式以建立信任

y

目錄

摘要

隱私中所謂的「暗黑模式(Dark patterns)」是一種欺騙性的策略，會誘導或操縱消費者提供更多超出他們意願的資料。許多企業即使明白事實上會侵蝕數位信任、增加風險及造成損害，卻仍然採用暗黑模式。本白皮書探討暗黑模式為什麼既常見且存在問題，並提供真實範例與因應策略，以支持更完善、更以消費者為中心的替代方案。

引言

許多消費者表示他們想保有隱私，但實際行為的結果通常卻事與願違。[1]這種自相矛盾的情形可能部分歸因於許多因素，包括缺乏對數位世界的認知或理解，以及在使用數位產品或服務之前，人們不願意閱讀冗長或複雜的隱私聲明。[2]這也可能歸因於限制個人資訊的蒐集和利用，或要求不被追蹤的難度。此外，人們他們每天還會遇到大量眾多的資料共享要求。因此，他們可能在歷經「疲於同意(Consent fatigue)」情況下接受這些請求，而未顧及是否符合其隱私偏好。[3]

許多網站和應用程式會在預設情況下追蹤使用者以提供更好的使用者體驗，但是選擇退出或限制追蹤可能會非常困難。

擁有複雜隱私設定和混亂隱私介面的企業往往會落入「暗黑模式(Dark patterns)」的陷阱。這些做法會嚴重影響企業信譽以及來自消費者的信任。然而，隱私專家能與使用者體驗(UX)設計者密切合作以避免這些顧慮，並為消費者創造真正以隱私為核心的體驗。

何謂「暗黑模式」

企業可能運用暗黑模式來誘騙或操縱消費者購買產品/服務，或放棄他們的隱私[4]。暗黑模式是會使系統/產品使用者難以理解與表達自己的隱私設定及偏好的一些做法。在某些情況下，開發人員會故意透過介面或功能設計，以引誘使用者消費或過度分享數據。

例如，美國聯邦貿易委員會(FTC)最近指控亞馬遜(Amazon)操縱消費者註冊成為會員期限自動展期之Prime會員。FTC列舉了亞馬遜蓄意使用的一系列暗黑模式，從未訂閱 Amazon Prime將難以購買商品，到誘騙消費者在完成交易時付費訂閱，以及故意建立一個複雜的取消訂閱流程。[5]

暗黑模式不僅僅是讓使用者花錢，它們還可能騙取使用者的個人資訊。隱私領域中的暗黑模式（本文亦稱「欺騙性模式」）是一種為欺騙或促使使用者做出與其隱私偏好不一致的行為所精心設計的手段。

1 John, L.; "We Say We Want Privacy Online, But Our Actions Say Otherwise," *Harvard Business Review*, 16 October 2015, https://hbr.org/2015/10/we- say-we-want-privacy-online-but-our-actions-say-otherwise

2 Griffith, E.; "Everyone Wants Data Privacy, But No One Reads Privacy Agreements," PC Mag, 19 April 2021, https://www.pcmag.com/news/everyone-wants-data-privacy-but-no-one-reads-privacy-agreements

3 Schermer, B.; B. Custers; S. Van der Hof; "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection," *Ethics and Information Technology*, vol. 16, iss. 2, May 2014, https://www.researchgate.net/publication/271922021_The_crisis_of_consent_How_stronger_legal_protection_may_lead_to_weaker_consent_in_data_protection

4 US Federal Trade Commission (FTC), "FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers," 15 September 2022, https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap- consumers

5 FTC, "Federal Trade Commission v. Amazon.com, Inc.," 21 June 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/amazon-rosca-public-redacted-complaint-to_be_filed.pdf

這些方法體現於：拙劣的使用者介面設計、難以尋找或理解的隱私設定、措辭模糊不清，以及耗時繁瑣的退出流程。

以隱私事件為例，2022年Google因涉嫌使用暗黑模式而被判賠8500萬美元，該訴訟指控Google即使在使用者關閉追蹤定位服務後，仍會在Android手機的後台環境中追蹤使用者位置。除此之外，相關指控也提到難以找到隱私設定。[6]

以上只是幾個例子，欺騙性模式的使用正在不斷增加[7]，企業必須阻止欺騙性模式成為常態或可接受的行為。懂得尊重使用者並使他們能夠表達隱私偏好的企業，將能夠贏得消費者的信任，比起不尊重資料擁有者的同行更具有競爭優勢。

為什麼暗黑模式如此常見？

許多企業相信數據是現代最重要的戰略資產，數據可以洞悉消費者購物的趨勢，並顯示出鎖定目標並投放行銷廣告，進而提升銷售收入的資訊。然而，在「越多越好」的錯誤理論下，一味追求更多數據，將導致增加對暗黑模式的依賴性。

依賴個人資訊量身打造廣告的行銷專家，並非隱私專家，他們可能完成企業全面性的隱私意識培訓，但內容主要聚焦於合規性，而非數位信任的建立。因此，隱私專家必須主導與行銷團隊的合作，協助平衡可能的利益衝突，使每個人皆能一同維護隱私權。

促使欺騙性模式層出不窮的不光是行銷團隊，任何會製作線上產品、服務或消費者會接觸到的內容(例如：網站設計)、撰寫電子郵件文案，或是開發應用程式的部門，都可能無意間使用到欺騙性模式。在許多企業裡，隱私專業人員可能沒有與這些部門合作，或是等到問題發生才介入，而隱私專業人員的參與不足，將使欺騙性模式有機可乘。

儘管全球隱私法律及法規有助於保障資料當事人的隱私權，但它們也可能促使企業採用欺騙性模式。根據一項估計，「一般資料保護規則(GDPR)」讓允許使用Cookie的通知增加近40%。[8]雖然看似無害，但這些通知往往是欺騙性模式的主要來源，例如沒有明確的「拒絕」按鈕。雖然法律及法規要求企業提供通知並取得同意以蒐集個人資料，但它們可能無意中促使企業更具創意性(或欺騙性)地蒐集資料。

儘管全球隱私法律及法規有助於保障資料當事人的隱私權，但它們也可能促使企業採用欺騙性模式。

值得注意的是，並非所有欺騙性模式都是蓄意的。例如：不良的使用者體驗設計，使用難以辨識的顏色，也可能導致暗黑模式的產生。雖然在蒐集新用途的數據以及新產品或服務發布之前，都應該執行隱私衝擊分析(Privacy Impact Assessment, PIA)，但促銷電子郵件或網站文案中仍然可能存在利用暗黑模式的情況。由於隱私團隊鮮少與文案編輯或網頁設計人員合作，因此這些模式可能無法被辨認或測試。

6 Weatherbed, J.; "Google will pay $85M settlement to Arizona to end user-tracking suit," The Verge, 5 October 2022, https://www.theverge. com/2022/10/5/23389331/google-settlement-arizona-user-tracking-privacy-suit

7 *Op cit* US FTC

8 Kretschmer, M.; J. Pennekamp; K. Wehrle; "Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web," *ACM Trans. Web*,vol. 15, iss. 4, Article 20, June 2021, https://www.comsys.rwth-aachen.de/fileadmin/papers/2021/2021-kretschmer-tweb-Cookies.pdf

為何企業應關注暗黑模式？

儘管欺騙性模式在業界普遍存在，企業仍應致力於建立並維護與消費者的信任。最好的狀況是，個人僅為自己被誘騙而提供個人資訊感到沮喪；最壞的情況則是，他們會轉向選擇提供相同或類似服務的其他供應商。

新制定的隱私法規特別規範「暗黑模式」的使用。美國方面，加州率先立法禁止運用暗黑模式來取得使用者對於提供個人資料的許可。[9]雖然歐盟《一般資料保護規則》(GDPR) 最初未提及暗黑模式，但立法者已表示將提供更多有關約束暗黑模式的法律指引。[10]最終，未來法律法規可能全面禁止使用暗黑模式，然而基於現有監管措施及明確的監管趨勢，企業應採取積極措施以因應趨勢。

預防欺騙性模式除了能強化資訊安全，也能給予其他企業目標與價值的支持。近年來，多元共融(Diversity, Equity, Inclusion, DEI)議題備受許多企業重視，根據調查，有 95% 的執行長表示在未來幾年DEI是公司的重要目標之一。[11]然而，若宣稱重視 DEI，卻又同時使用欺騙性模式，將顯得自相矛盾。

欺騙性模式更容易對弱勢團體造成損害，尤其是收入較低和教育程度較低的人們。[12]

享有隱私權不應以高學歷或技術能力為前提。

以英語為母語的國家，暗黑模式可能會對技術知識較少和非母語人士造成不成比例的影響。[13]

享有隱私權不應以高學歷或技術能力為前提，企業必須努力為普羅大眾提供平等的機會，讓他們能夠根據自己的隱私偏好做出選擇。

「欺騙性模式」實務案例

欺騙性模式可能顯現在使用者體驗的不同階段和多種形式上。以下是一些常見的欺騙性模式及其應對方式。

具誤導性的 Cookie 通知

許多網站會在訪客造訪時，要求訪客同意蒐集Cookie。這些Cookie通知應該簡潔明瞭，並使用通俗易讀的語言。

9 The California Privacy Rights Act of 2020, https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

10 Cooper, D.; S. Jungyun Choi; J. Ong; A. Oberschelp de Meneses; "The EU Stance on Dark Patterns," Inside Privacy, 31 January 2023, https://www.insideprivacy.com/eu-data-protection/the-eu-stance-on-dark-patterns/

11 Hawkins, D.; "How CEOs Can Make Diversity And Inclusion A Priority," *Forbes*, 13 July 2022, https://www.forbes.com/sites/forbescoachescoun- cil/2022/07/13/how-ceos-can-make-diversity-and-inclusion-a-priority/?sh=463abf3e279a

12 Busch, K.; "What Hides in the Shadows: Deceptive Design of Dark Patterns," Congressional Research Service, 4 November 2022, , https://sgp.fas.org/crs/misc/IF12246.pdf

13 Germain, T.; "New Dark Patterns Tip Line Lets You Report Manipulative Online Practices," Consumer Reports, 19 May 2021, https://www.consumerreports.org/digital-rights/dark-patterns-tip-line-report-manipulative-practices-a1196931056/

「隱私及電子通訊指令(ePrivacy Directive)」是《一般資料保護規則 (GDPR)》的補充法規，要求網站在使用者瀏覽器儲存Cookie(僅嚴格必要性的 Cookie 除外) 之前，必須取得使用者的許可。[14]

由於缺乏如何撰寫Cookie通知的監管指引，因此欺騙性模式在Cookie通知中相當常見。

圖1 表示一項具誤導性 Cookie 通知的範例。

圖1：具誤導性的Cookie通知

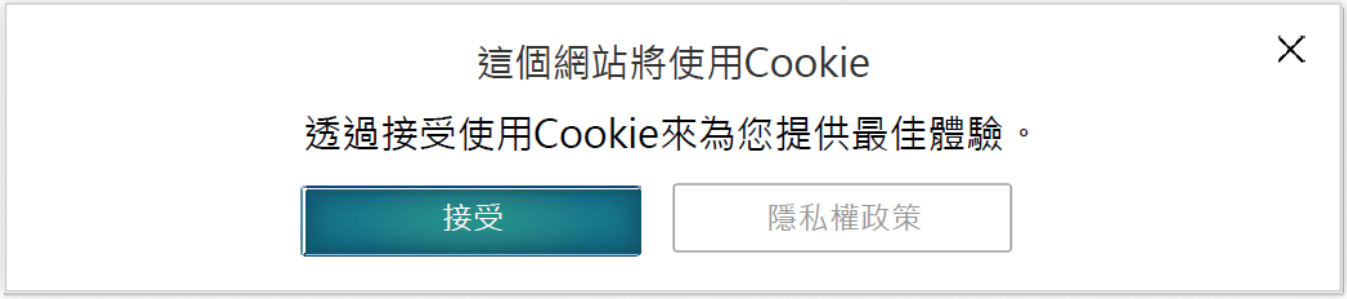


圖1的Cookie通知具有誤導性，可能會導致使用者對正要被蒐集的資訊做出不準確的決策。上圖未有明顯的「拒絕」按鈕，讓使用者誤以為他們只能接受Cookie追蹤，或閱讀隱私權政策後再接受Cookie追蹤。

就算「隱私權政策」按鈕裡可能含有拒絕Cookie的選項，許多使用者也未必會知道或願意為了停用追蹤而調整設定。

為了應對這種欺騙性模式，企業應確保 Cookie 警示標語盡可能易於理解。除了「接受」按鈕外，仍應有一個「拒絕」Cookie 的按鈕。

這個按鈕的文字要讓使用者明白，他們不需要接受 Cookie 就能使用網站，並確保按鈕的外觀看起來可以點選；有些Cookie 訊息視窗會將「拒絕」按鈕設為灰色，讓人誤以為無法點選。

多步驟 Cookie 提示視窗

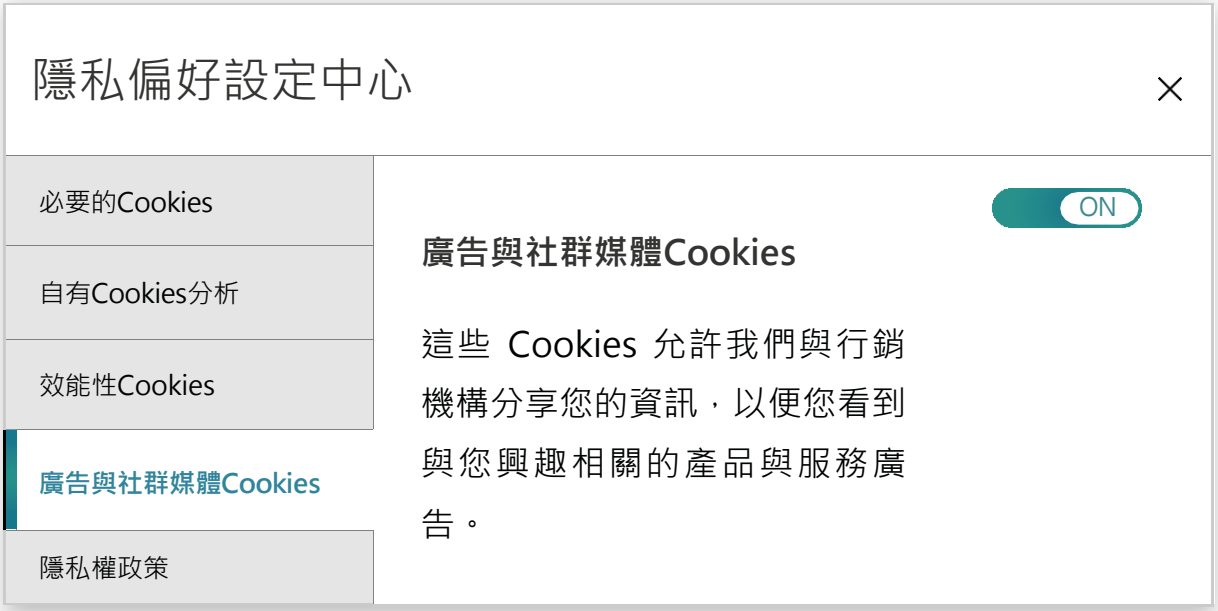
一些 Cookie 訊息欄要求使用者多次點選才能拒絕 Cookie，而接受 Cookie 則只需要點選一次。雖然幾次點選看似微不足道，但通常故意設計額外的點選時間和繁瑣的操作流程，是為了引導使用者走向隱私保護較少的路徑。**圖2** 顯示必須多次點選才能拒絕 Cookie 的訊息視窗。

網站訪客可能會對於**圖2** 中的Cookie 視窗感到失望，因為它需要至少四次點選（不包括切換按鈕）才能更改預設值設定。

若拒絕追蹤需要點選多次，但接受所有追蹤僅需點選一次，許多使用者可能會選擇接受所有 Cookie 追蹤，而不是在多個頁面上花時間設定及確認他們真實的隱私偏好。

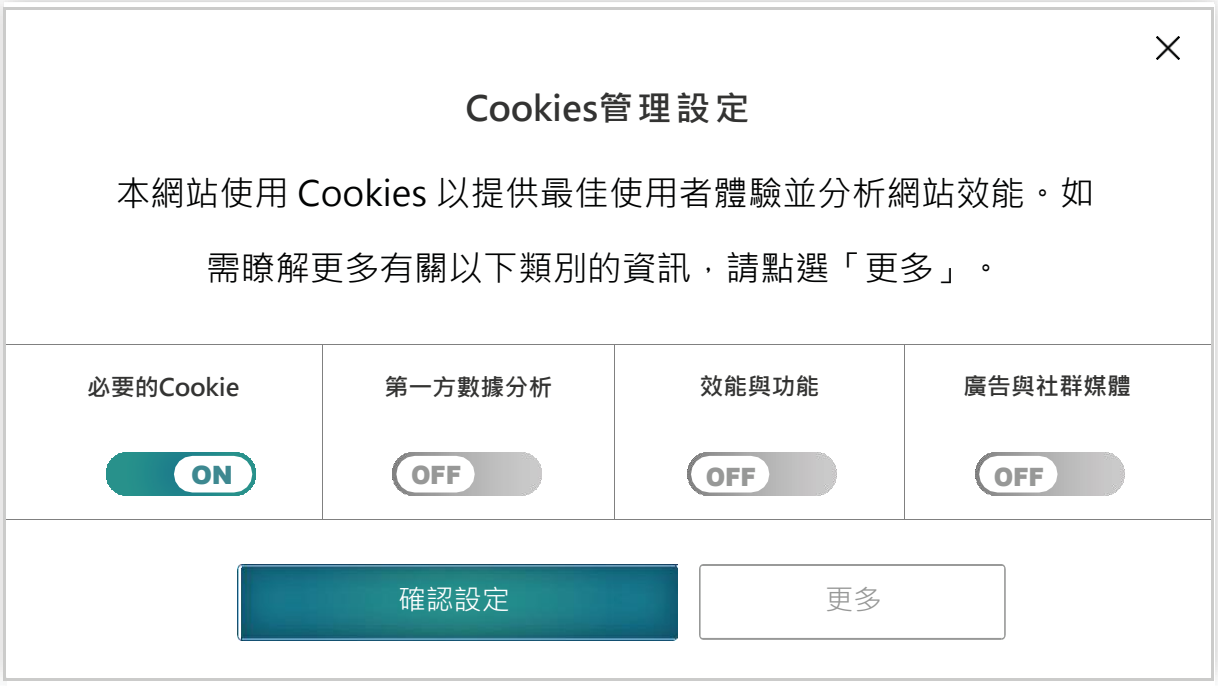
14 GDPR.EU, "Cookies, the GDPR, and the ePrivacy Directive," https://gdpr.eu/Cookies/

圖2：多步驟 Cookie 提示視窗



提供更為細緻的 Cookie 偏好設定固然有其價值，但呈現資訊的方式可以做得更好。在初始的 Cookie 訊息視窗中，透過每個追蹤類別的核取方塊，使用者能以更少的點選次數完成選擇。**圖3** 表示一個允許網站訪客表達其 Cookie 追蹤選項的訊息視窗，而無需點選多個標籤或選單。此外，多餘的追蹤選項在預設值設定中會被取消勾選。

圖 3: Cookie 視窗類別設定



複雜的隱私設定

Cookie 視窗只是暗黑模式顯現的一部份，它們也可能出現在複雜且難以瀏覽的選單中，並且將隱私設定隱藏起來。擁有可存取的隱私設定至關重要，因為隱私通知通常會因為長度和密度而被忽略。平均每位美國人手機上有 80 個行動應用程式 (app)。[15]

閱讀所有相關的隱私政策需要 22.4 小時[16]，這還不包括瀏覽過的網站。面對這些挑戰，相較於閱讀冗長的隱私政策，使用者可能會偏向易於修改隱私設定的選擇。[17]因此，企業必須讓隱私設定容易被找到，這一點至關重要。

隱私設定可以透過以下方式隱藏：

- 在偏好設定頁面中只有一個很難發現的標籤，讓使用者透過它去修改設定。
- 隱私設定放在沒有提及隱私的頁面中（例如，安全設定頁面）。
- 與隱私相關的設定分散在多個偏好設定頁面中，而非位於使用者易於修改的設定中心。

針對此議題最有效的解決方案之一，是提供使用者多種路徑存取隱私設定。[18]例如，隱私設定頁面可以透過使用者個人檔案頁面、設定頁面，以及網頁底部之隱私連結進行存取。另外，建立包含存取隱私設定提示的常見問答集，以及訓練客服人員協助使用者如何查找設定，亦是非常值得執行的措施。

缺少設定介面的物聯網裝置

物聯網 (IoT) 裝置，例如運動追蹤器和智慧家電，有時會蒐集精細且敏感的資訊。然而，由於許多物聯網裝置不像手機和電腦具備螢幕，因此使用者可能不容易存取隱私設定，甚至可能缺乏處理隱私偏好的機制。事實上，部分物聯網裝置甚至沒有隱私政策。（可能會有針對產品網站或相關應用程式的政策，但並無針對裝置及其所蒐集數據的特定政策。）

圖4 說明了一些常見的物聯網裝置類別、可能蒐集的數據以及根據所蒐集的數據對使用者所下的推論。請注意，物聯網裝置蒐集的數據可能因不同裝置而異。

圖 4：物聯網(IoT)裝置與其蒐集的資料

物聯網裝置類別	蒐集的資料	根據資料所做出的推論
運動追蹤器	心率、睡眠模式、步數	一個人的心率資料可能反映其壓力水準，隨著時間的趨勢中可能透露出此人的日常活動內容，例如何時睡眠等。
影像門鈴	影像錄製、語音錄製	影像錄製可能會擷取到鄰居和訪客的臉部特徵，這些影像可能會被分享給地方執法機關。
娛樂串流裝置	觀看的頻道/節目、串流時長	觀看的頻道/應用程式可能顯示家庭人口統計、興趣和政治觀點。
電子書閱讀器	購買的書籍與其位置	購買的書籍可能透露個人性向、政治信仰或健康狀況等資訊。

15 Flynn, J.; "40 Fascinating Mobile App Industry Statistics [2023]: The Success of Mobile Apps in the U.S.," Zippia, 2023年3月20日, https://www.zippia.com/advice/mobile-app-industry-statistics/#:~:text=The%20average%20American%20has%2080,app%20downloads%20worldwide%20in%202020

16 Fowler, G.; "I tried to read all my app privacy policies. It was 1 million words.," *The Washington Post*, 31 May 2022, https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/

17 Tkacik, D.; "Finding privacy choices on websites is hard for average users.," CyLab, 11 June 2020, https://www.cylab.cmu.edu/news/2020/06/11-privacy-choices-websites.html

18 *Ibid.*

從物聯網裝置所收集到的資料能揭露許多資訊並得出結論，當消費者在初始化設定物聯網裝置，以及之後的使用過程中，能夠輕易修改隱私權的設定，是極為重要的。

此外，企業應針對裝置、相關的應用程式和網站制定個別的隱私權政策。僅有針對物聯網裝置的應用程式的政策是不充分的，還須凸顯出由裝置所蒐集及使用的資訊。

操縱性/令人困惑的語言

有些資訊請求依賴操縱性語言。例如，零售網站可能會要求客戶提供電子郵件地址以接收促銷電子郵件，客戶可輸入其電子郵件地址或點擊類似「我討厭省錢」的連結（**圖5**）。除操縱性語言之外，使用者也可能不清楚是否可以在不提供電子郵件地址的情況下進入該網站，因為拒絕的選項顯然不是一個按鈕。

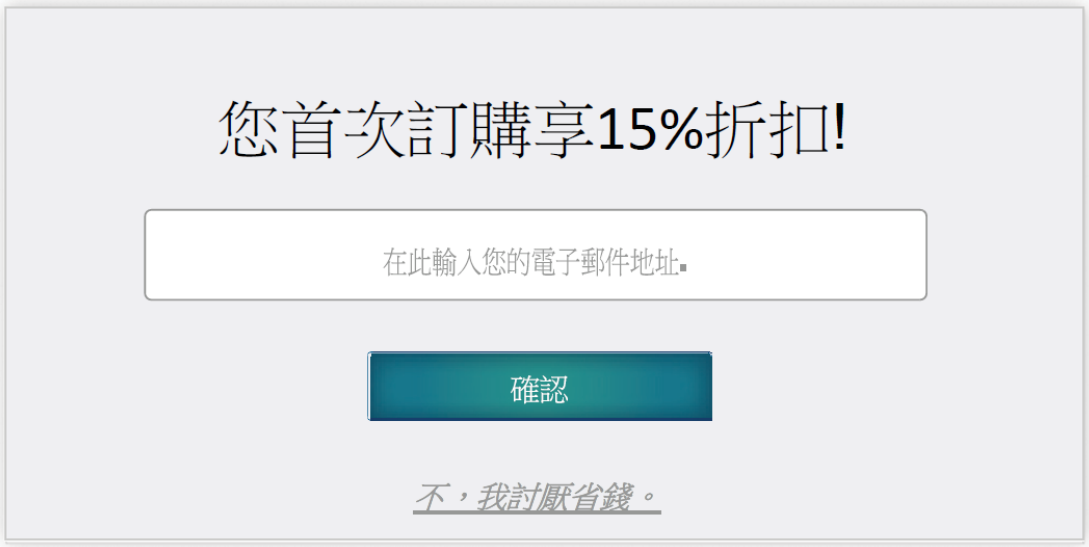
有些許可之要求利用令人困惑的語言來操縱使用者，讓使用者不清楚要同意什麼。透過清楚地表明使用者無需提供電子郵件地址即可進入網站，可避免這種欺騙性模式，這意味著讓「拒絕」按鈕像分享資訊按鈕一樣顯而易見。

此外，「不提供資訊」的選項，不應帶有任何評斷；例如，一個透過其他詞彙來取代「拒絕」的按鈕，允許使用者在沒有任何壓力的情況下選擇不分享資訊。

此暗黑模式還可能需要將必要的功能性 Cookies 與選擇性追蹤的 Cookies 組合在一起，以致使用者認為此類追蹤對於網站的正常運作是必要的。

為避免導致欺騙性模式的困惑性語言，應確保負責建立此複本的部門與隱私及使用者體驗團隊共享複製本以供審核。

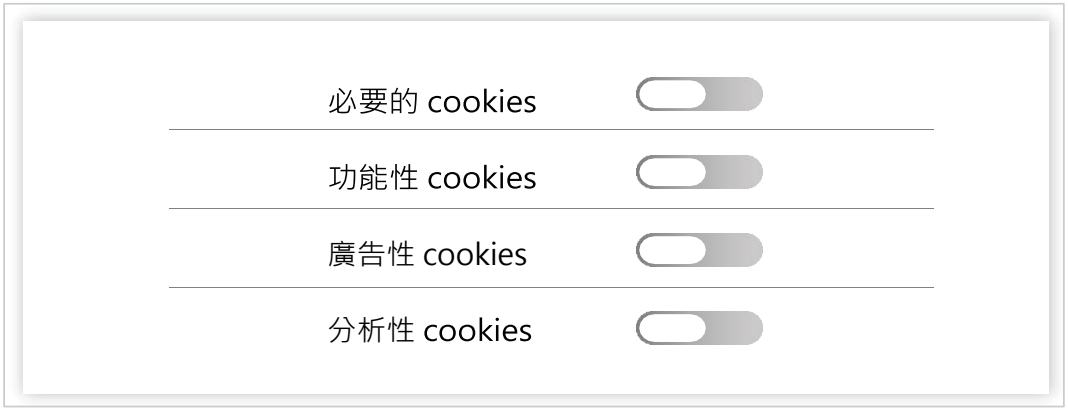
圖 5：電子郵件蒐集請求中的操縱性語言範例



不良的介面設計

與隱私相關網路介面的設計方式可能會故意誘騙使用者分享其個人資訊，當各種切換難以理解或缺乏對比時可能會發生這種情況。由於**圖 6** 中的切換開關沒有使用強烈的對比或鮮明的顏色來表示什麼是允許的或什麼是不允許的，所以使用者可能很快看一眼便以為功能性、廣告性和分析性 Cookies 是不被追蹤。

圖 6: 令人困惑的切換

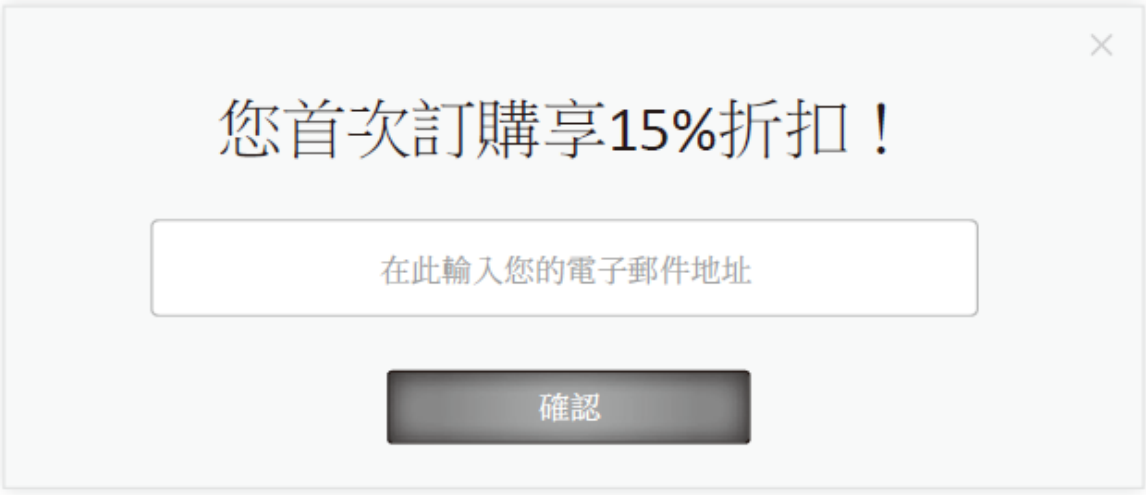


為解決這種欺騙性模式，要確定切換是使用顏色來表示何時啟用追蹤。在任何啟用的切換旁邊加“打開”一詞也可能有用，可讓使用者確認已做出選擇。

不良的介面設計也包含彈出視窗中顯示難以看到的「關閉」按鈕。 **圖7** 顯示彈出視窗右上角有一個難以看見的小“x”。由於幾乎沒有對比，使用者可能不知道提供電子郵件地址是可選的，並且可能認為需要提供才能造訪該網站。透過使用更多的對比、利用使用者體驗最佳實踐以及在部署上線之前進行廣泛的測試來輕易解決該情形。

圖 7: 關閉的按鈕

有些介面對於在Cookie訊息視窗中所選的是甚麼選項也不清楚。例如，如果「接受」及「拒絕」被點選後會變色，則可能不清楚變色是否表示被選中。為解決此問題，要讓使用者清楚選擇了哪個選項，這可在使用顏色之外加上文字以消除任何模糊不清的情形。



電子郵件取消訂閱連結常常蓄意地利用不良的設計來讓使用者保持訂閱，某些促銷電子郵件的訊息中可能不包含容易找到的取消訂閱連結。此外，取消訂閱頁面有時會利用令人困惑的措辭，以致難以選擇退出後續的對話。

例如，電子郵件的取消訂閱頁面可能會顯示“您確定要取消訂閱嗎？”並以“否”作為突出醒目的選項，“是”則在下面且字體較小。為解決這種暗黑模式，要確定所有選項都經過類似的設計處理，並且顏色不會促使使用者做出某種選擇。

強制註冊

強制註冊要求使用者建立帳戶並提供個人資訊才能存取資訊、服務或產品。雖然完成交易可能需要某些資訊，例如用於訂單確認的電子郵件地址，但企業不應要求使用者建立帳戶。

若因某些原因，需要讓使用者建立帳戶時，要限制蒐集的資訊量。例如，不要求使用者在其帳戶中儲存信用卡資料，如果產品不需郵寄給使用者，則不要求實體郵寄地址等。若要求使用者建立帳戶，則應清楚解釋將如何使用這些資訊。.

無法更改設定

有些企業讓隱私相關的設定很難予以更改，這些設定或許會清晰呈現，但使用者無法修改它們，例如，需要有電子郵件地址才能下載資源（**圖 8**）。

圖 8 中的要求被視為隱私暗黑模式，因為它強迫使用者向第三方分享其資訊。

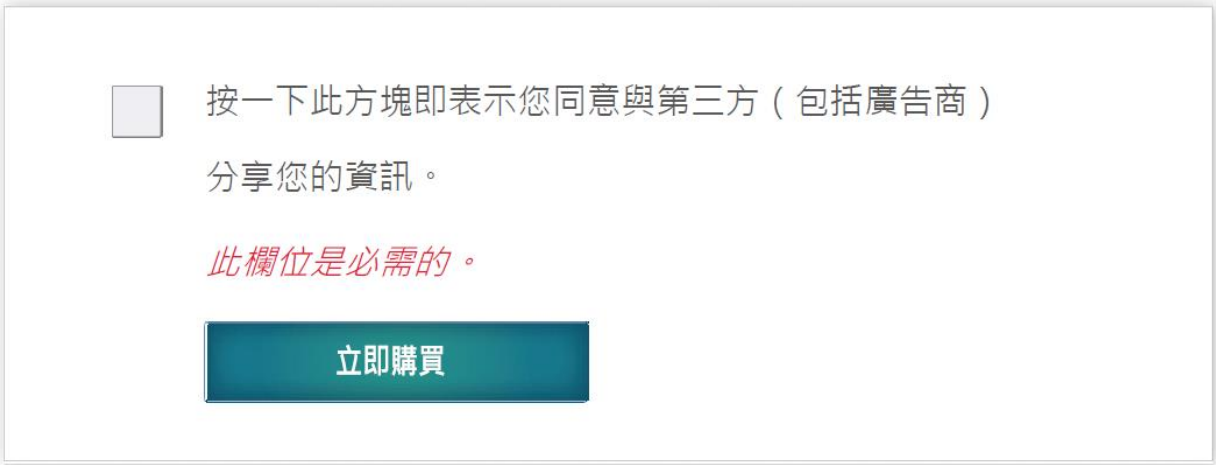
與第三方分享資訊對於使用者進行購買的功能性並非必要。 因此，在此情況並無正當理由向第三方分享資訊。

有些網站還利用無法更改設定來進行 Cookie 追蹤，例如：Cookie 訊息視窗可能只有接受 Cookies 或「了解更多」的選項，而「了解更多」的連結並不提供使用者選擇退出追蹤的方式。

這與涉及令人困惑的 Cookie 訊息視窗的欺騙性模式不同，因為令人困惑的 Cookie 訊息視窗仍允許使用者選擇退出追蹤。

為解決此暗黑模式，應實現資料最小化原則。亦即：蒐集最少量的必要資訊。企業必須知道各服務項目需要什麼資料以及這些資料將如何使用。而不應蒐集多餘的數據。

圖 8：無法更改設定



預設值設定

有些企業倚仗著資料當事人對預設的隱私設定不知如何更改或不關心，預設值設定可能是不保護隱私，不更改設定的使用者可能會被分享較他們所預期更多的資訊。

如果圖8中的複選框是被自動選中，非隱私保護的欺騙性模式的預設值設定將會是典型的例子。透過設計以實踐隱私，將有助於減少預設值設定所導致的暗黑模式。

解決欺騙性模式

隱私暗黑模式普遍存在且可能存在於企業與個人之間的大量互動中。隱私設計及跨職能協同合作有助於防止欺騙性模式並限制對資料當事人的傷害無法更改設定。

隱私設計

隱私設計，將全部的隱私納入整個開發生命週期（包括建置及使用），有助於解決暗黑模式並限制非故意的欺騙性設計所造成的危害，以下是隱私設計的七項原則：[19]

- **積極主動，而非被動反應；預防性而非補救性** - 隱私專業人員應在收到投訴前修復暗黑模式；那時，信譽受損及信任喪失已經發生，而且可能無法挽回。反而應透過與其他部門合作以及對新開發的隱私衝擊分析，主動辨識及消除任何暗黑模式。
- **隱私作為預設值設定** - 如果系統及網站被配置為預設保護隱私，則非故意的暗黑模式造成的危害將是有限的。即使使用者很難找到或修改他們的隱私相關設定，他們的追蹤偏好也應是預設為保護隱私，並且需要使用者進行操作，才得以分享資訊。 操作要依資料當事人需要選擇資料分享而非選擇退出資料分享的心態進行。
- **嵌入設計中的隱私** - 隱私專家可以尋求使用者體驗設計者的協助，以確保設計中的使用者偏好將隱私納入考量。此原則包含消費者可以設定自己的隱私偏好以及系統及產品預設蒐集的資料。這項原則有助於消除與強制註冊、物聯網介面限制、不良的介面設計以及隱私相關設定之呈現等相關聯的暗黑模式。
- **全功能性：正和而非零和** - 這項原則可以確保可用性、功能性及獲利力與隱私相容。增強的隱私必須與業務目標相容，最終，隱私應該是一個核心功能考慮因素。系統及網站應設計成以最少且必要的使用者資訊來進行運作。這項原則可以幫助消除與物聯網介面、強制註冊和無法更改設定相關聯的暗黑模式。
- **端到端的安全：全生命週期保護** - 此原則確保消費者提供的資訊得到充分保護。如果暗黑模式蒐集的資料超出了絕對必要的範圍，強大的安全措施可以保護企業擁有的資訊，限制對個人的傷害。
- **能見度及透明度：保持開放** - 暗黑模式與此原則背道而馳。保持誠信及透明的企業對所蒐集的資料及這些資料的使用方式不能利用欺騙性模式。應注意，此透明度不僅涉及使用者看到的前端；還涉及使用者看不到的後端發生的資料處理及共享。 這項原則有助於解決與操縱性語言及令人困惑的 Cookie訊息視窗相關的欺騙性模式。
- **尊重使用者隱私：保持以使用者為中心** - 設計時心中要有使用者（而非僅是她們資料），確保個人可以表明他們的隱私偏好並採取行動保護他們的隱私。最後，所有蓄意的欺騙性模式都可透過尊重使用者及在設計時心中有他們來得到修正。

19 Cavoukian, A.; "Privacy by Design—The 7 Foundational Principles," January 2011, https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

了解使用者

解決欺騙性模式需要了解企業的使用者或潛在使用者是誰。他們的能力、偏好及背景將大大地影響企業如何履行其隱私義務及各項設定。**圖 9** 包含一些人口統計資訊及相關隱私的考慮。

圖 9：人口統計資訊及隱私的考慮因素

人口統計資訊	對隱私的影響
年齡	• 處理未成年人的資料可能需要額外的隱私考量。 • 生於數位環境的人可能會發現，與那些沒有數位科技伴隨成長的人相比，他們更容易存取及修改設定。
宗教	• 來自某些地區的使用者可能需要額外的隱私考量。 • 隱私權聲明可能需要以多種語言提供，以確保所有使用者都能理解。 • 文化因素可能會影響隱私設定的整體外觀與設計（例如，某些顏色的文化內涵）。
能力	• 隱私設定必須考慮可存取性（例如，適應色盲）。 • 隱私權聲明必須以有意義且易於理解的方式傳達給使用者。

大多數人口統計資訊可以從分析與績效衡量程序中取得，為了解使用者，隱私專業人員必須獲得使用者體驗團隊的協助。

協同合作：消除暗黑模式的關鍵

隱私專業人士無法單方面消除暗黑模式。然而，透過與使用者體驗及行銷部門密切合作，隱私團隊可幫助減少這些模式的出現。

UX(使用者體驗)

使用者體驗專業人員對企業使用者有寶貴的洞察力，他們確保設計的使用者友善性並充當使用者之倡導者。

隱私專業人員時常與資訊安全、法律與合規以及風險管理團隊密切合作，但只有三分之一的隱私專業人員總是或經常與產品/業務開發團隊合作。[20]隱私專業人士及使用者體驗專業人士都需要考慮使用者：隱私權團隊考慮隱私角度，而使用者體驗團隊則考慮使用者的體驗。他們可以隱私為中心的方式共同優化使用者的旅程。此外，使用者體驗團隊可以幫助確保隱私不被用來交換功能，反之亦然。

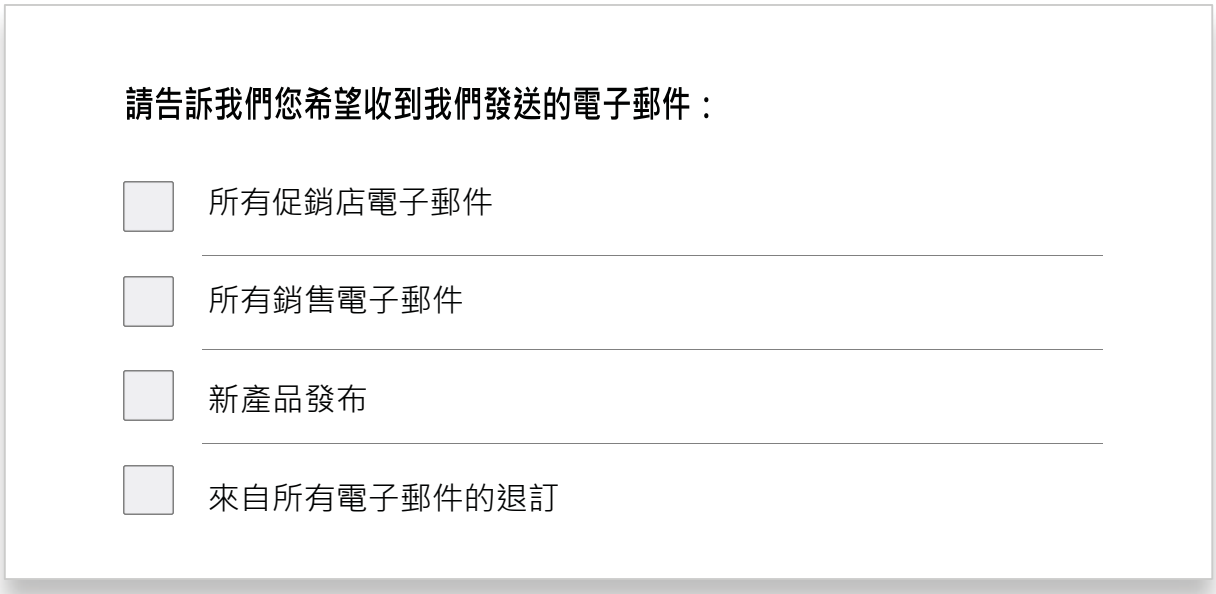
行銷

行銷專業人士業人士通常需要大量有關既有的及潛在客戶的資訊，這可幫助他們將廣告內容定位到更有可能採取行動的個人，但在不欺騙人們放棄他們的資訊觀點的情況下獲得這種洞察力是可能的。

圖10 顯示了一個電子郵件偏好選框，允許使用者表示他們希望接收哪種類型的通訊。除了允許使用者清楚地表明他們的偏好之外，這種方法還可以提高參與度，因為使用者自我確認自己的興趣，而不是行銷人員依據追蹤所假設的興趣。

20 ISACA, Privacy in Practice 2023, 2023, https://www.isaca.org/resources/reports/privacy-in-practice-2023-report

圖 10：選擇接收行銷電子郵件



隱私專業人士應該向行銷團隊強調，無論有意或無意，以欺騙方式取得同意追蹤，可能會適得其反。

隱私專業人士還必須教育行銷人員了解操縱性複本可能造成的危害以及為什麼它在消費者眼中構成欺騙性模式。欺騙人們提供個人資料所帶來的任何暫時收益，都可能會被消費者長期失去信任所抵消。強調滿足合規性要求是最低要求，而獲得信任可能需要超越合規性要求。

簡化使用者的隱私體驗

使用者體驗是指以有用的方式為使用者創建產品的方法。[21] 使用者體驗對用戶的關注使其可與隱私設計上相輔相成，而隱私工程應該是以使用者為中心。企業的使用者體驗部門對使用者有很多洞察力，這對隱私資訊的傳達方式與隱私設置的呈現方式可有極大地的影響。

而使用者體驗專業人員聚焦於使用者，隱私專業人員也應該這麼做。作為使用者的倡導者，可以確保業務實踐與介面設計對使用者友善。 與使用者體驗專業人士一起工作，隱私專業人士可能需要爭辯似乎與某些業務期望不一致的實務處理及原則。雖然可能需要做出妥協，但隱私專業人士可確保他們的企業預設值為保護隱私。

欺騙人們提供個人資料所帶來的任何暫時性收益都可能會被消費者長期失去信任所抵消。

由於 53% 的技術隱私專業人員稱其企業人員有些或嚴重不足，[22] 期望隱私專業人員將其專業知識傳授給每個開發項目是不可行的。

雖然如此，隱私專業人士可以向開發及使用者體驗團隊傳授有關隱私的知識，以幫助確保在未來專案的設計中納入考慮。

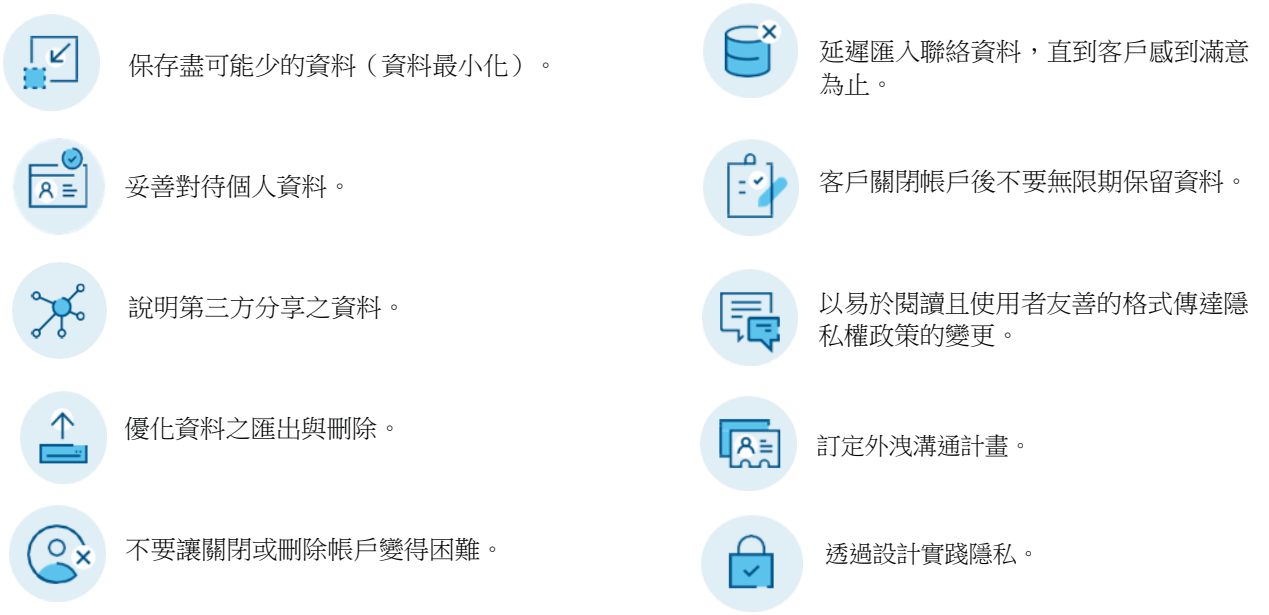
21 Interactive Design Foundation, "User Experience (UX) Design," https://www.interaction-design.org/literature/topics/ux-design
22 *Op cit* ISACA

以下是隱私專業人士向使用者體驗設計者強調的一些要點：

- 表示不希望被追蹤的點擊次數應與同意追蹤的點擊次數相同。
- 預設值設定應該是蒐集最少量的必要資訊。
- 使用者無需採取任何行動即可保護其隱私。
- 誘騙人們表示同意可能會造成代價高昂的後果。
- 有些資訊被視為個人資訊，並且可以從企業蒐集的資訊中得出某些結論（例如，位置資料如何揭露一個人的醫療狀況）。
- 可能存在隱私合規問題以及懸而未決的隱私相關法律訴訟。

使用者體驗設計者可能熟悉隱私認知設計框架，這是一組有助於促進考慮隱私的設計的指南。**圖11**顯示了隱私認知設計框架。[23] 此框架可作為隱私團隊與使用者體驗設計者之間對話的起點。

圖 11：隱私認知設計框架



中小企業的欺騙性模式

較小或較新的企業可能沒有使用者體驗人員，或者使用者體驗設計者可能沒有足夠的資源與隱私團隊合作。 在這種情況下，想要倡導使用者體驗的隱私專業人士可以在《網頁內容可存取性指南(WCAG)》[24]中找到有關良好設計的指南。WCAG對於如何確保人們可依其不同需求來存取使用內容並移除因視覺設計不佳而導致的欺騙性模式（例如，難以閱讀的切換或缺乏對比），提供了指引。

小型企業的隱私專業人員可能比大型企業的隱私專業人員更具優勢，因為會製作面對消費者內容及資源的部門較少。在許多大型企業中，隱私專業人員無法與企業各部門蒐集資料的人員會面，並確保他們不使用暗黑模式。相較之下，小型企業的隱私專業人員可以更深入地了解各個部門（例如行銷、人力資源及財務）蒐集及使用的資料。

23 Friedman, V.; "Privacy UX: Privacy-Aware Design Framework," *Smashing Magazine*, 25 April 2019, https://www.smashingmagazine.com/2019/04/privacy-ux-aware-design-framework/

24 Web Content Accessibility Guidelines, "Designing for Accessibility," https://wcag.com/designers/

隱私專業人員應考慮到需修改隱私設定的使用者，由於資源有限，為每個潛在資料當事人進行設計是不可能的。因此，為新消費者（即不熟悉企業及其應用程式或網站設定的人）而設計很有用。奇特的是，如果隱私設定是在設計時考慮到新使用者，那麼有經驗的使用者很可能也能夠駕馭它們。

付諸實踐

在理想情況下，企業將消除所有暗黑模式，但使用者體驗與隱私團隊在鼓勵其他部門控制欺騙性模式時可能會遇到一些阻力，許多商業模式無意中依賴欺騙性策略來蒐集及處理資訊。隱私專業人士不應在支援資料當事人方面妥協。企業領導階層可能會做出與隱私權背道而馳的決策，但隱私專業人士有責任讓企業注意到欺騙性模式及其可能帶來的衝擊。

當倡導消除暗黑模式時，引用相關的法律及採取行動是可能有幫助的；這有助於量化未能解決暗黑模式時的金額損失。它可作為隱私影響評估或資料保護影響評估的一部分來完成，這可能是依據司法管轄對企業的一項要求。[25]解釋使用暗黑模式所帶來的損害，傾聽依賴欺騙性模式的部門之擔憂，並探討是否有辦法讓他們蒐集所需要的資訊而不需欺騙資料當事人。

結論

許多企業嚴重依賴隱私暗黑模式來追蹤客戶，但那些主動解決暗黑模式並遵守消費者隱私偏好的企業可以獲得競爭優勢。僅靠隱私專業人士無法消除企業的暗黑模式，他們必須與其他部門密切合作，創造面向消費者的產品、服務、網站及內容。隱私專業人士應該注意他們在個人生活中遇到的欺騙式模式，並確保他們的企業也不會使用到。努力糾正迫使使用者放棄隱私的設計有助於與消費者建立數位信任，從而帶來許多好處，包括良好的信譽、更可靠的決策資料以及較少的隱私外洩及網路安全事件。[26]

25 GDPR.EU, "Data Protection Impact Assessment (DPIA)," https://gdpr.eu/data-protection-impact-assessment-template/#:~:text=A%20Data%20Protection%20Impact%20Assessment%20(DPIA)%20is%20required%20under%20the,help%20you%20execute%20the%20assessment

26 ISACA, State of Digital Trust 2023, 2023年, https://www.isaca.org/digital-trust/state-of-digital-trust

致謝

ISACA認可並致謝：

專業評審員

Yunique Demann
CISA, CISM, CDPSE, CCISO, CIPT, CISSP
USA

Kevin Fumai
CDPSE, CIPP/US/E, CIPM, CIPT, FIP, PLS, CCSK, CEET
USA

Larisa Gabudeanu
CISA, CISM, CRISC, CDPSE
University Babes-Bolyai, Romania

Mathew Holdt
CISA, CIA, CFE
Protiviti, USA

Ng Wai Hou
CDPSE
Macau

Roy Marra
CRISC, CDPSE
IESO, Canada

Peter Matavovszky
CISM
Switzerland

Ryan W. McCuskey
McCuskey LLP
USA

Nandita Rao Narla
CISA, CISM, CRISC, CDPSE, CIPM, CIPP/US,CIPT, FIP
USA

Kane Porter
CISA, CIPP/C
Canada

Juan Pablo Barriga Sapiencia
CSX-P, CDPSE, CompTIA (A+, Network+, Security+) LPIC-1
Bolivia

董事會

John De Santis, Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Brennan P. Baybeck, Vice-Chair
CISA, CISM, CRISC, CISSP
Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Stephen Gilfus
Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP, NACD.DC
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, France

Gabriela Hernandez-Cardoso
NACD.DC
Independent Board Member, Mexico

Jason Lau
CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP
Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo
Independent Director, Former Chief Executive Officer and Executive Director, VADS Berhad Telekom, Malaysia

Maureen O'Connell
NACD.DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

Erik Prusch
Chief Executive Officer, ISACA, USA

Pamela Nigro
ISACA Board Chair 2022-2023
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

Gregory Touhill
ISACA Board Chair 2021-2022
CISM, CISSP
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

關於 ISACA

ISACA® (https://www.isaca.org/) 是一個推動個人與組織追求數位信任的全球性社群。 50 多年來，ISACA 為個人與企業提供知識、證書、教育、培訓與社群，以促進其職涯發展、改造其組織並建立一個更值得信賴及合乎倫理道德的數位世界。 ISACA 是一個全球性專業協會與學習型組織，擴展其在資訊安全、治理、保證、風險、隱私及品質等數位信任領域工作的170,000 名成員的專業技能。它已在全球 188 個國家共設立225 個分會。 ISACA 透過其 One In Tech 基金會，為資源不足及代表性不足的人們提供 IT 教育與職涯發展途徑之支援。

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

免責聲明

權利保留

Provide Feedback: www.isaca.org/eliminating-deceptive-privacy-practices

Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums

Twitter: www.twitter.com/ISACANews

LinkedIn: www.linkedin.com/company/isaca

Facebook: www.facebook.com/ISACAGlobal

Instagram: www.instagram.com/isacanews/

中文版致謝名單

ISACA台灣分會葉奇鑫理事長

翻譯(按姓名筆劃): 呂伯雲、林煒傑

校稿: 邵之美

編輯排版: 游恬欣