DIS SIRI, DIS XIAO, QUE FAITES-VOUS DE MES DONNEES PERSONNELLES ? » INFLUENCE D'UN PRIVACY SCORE SUR L'INTENTION D'ACHAT D'UN OBJET CONNECTE : LE CAS DES ENCEINTES CONNECTEES

Résumé : Cette recherche étudie l'influence d'un score indicatif du respect de la vie privée (*privacy score*) sur l'intention d'achat d'un objet connecté (enceinte connectée) et teste comment la marque, selon son niveau de crédibilité, modère cette influence. Au moyen d'une expérimentation en ligne, menée auprès de répondants représentatifs de la population française (n = 268), nous montrons que ce score a un effet direct et indirect (*via* la vulnérabilité perçue) sur l'intention d'achat. La marque influence directement l'intention d'achat mais modère également la relation entre le *privacy score* et l'intention d'achat. L'expertise technologique perçue a quant à elle un effet direct sur l'intention d'achat, mais aussi un effet indirect au travers de la préoccupation pour la vie privée (situationnelle) et de la vulnérabilité perçue. Nous recommandons aux marques, surtout à celles souffrant d'un manque de confiance de la part des consommateurs, d'intégrer l'affichage d'un *privacy score* favorable afin de diminuer le sentiment de vulnérabilité et d'augmenter l'intention d'achat. Quant à celles qui bénéficient de la confiance des consommateurs, leurs efforts marketing pour obtenir cette crédibilité ne sont pas vains puisqu'ils permettent de contrer l'effet d'un *privacy score* défavorable.
Mots clefs : Objets connectés ; Vulnérabilité ; *Privacy concern* ; Confiance ; *Privacy score*

"*HEY SIRI, HEY HIAO, WHAT DO YOU DO WITH MY PERSONAL DATA?*": THE INFLUENCE OF A PRIVACY SCORE ON INTENTION TO BUY CONNECTED OBJECTS – THE CASE OF SMART SPEAKERS

Abstract: This research aims to investigate the effect of a privacy score on the intention to purchase a connected object (smart speaker). It also looks at how the brand, depending on its credibility level, moderates this effect. Using an online experiment, conducted with respondents representing the French population (n = 268), results show a direct and indirect effect (*via* perceived vulnerability) of this score on purchase intention. Furthermore, the brand directly influences purchase intentions but also moderates the privacy score-purchase intentions relationship. Regarding the effect of perceived technological expertise, it has a direct effect on purchase intention, but also an indirect effect through privacy concern and perceived vulnerability. We then recommend brands, especially those with a low level of consumer trust, to display a favorable privacy score in order to decrease perceived vulnerability and to increase purchase intentions. Concerning firms with high levels of consumer trust, their marketing efforts to obtain this credibility are not useless since they can attenuate the effect of an unfavorable privacy score.
Keywords: Connected Objects; Vulnerability; Privacy concern; Trust; Privacy score

Introduction

Les objets connectés (OC) ont envahi notre quotidien et font désormais partie intégrante de nos modes de vie. Pourtant, pour fonctionner pleinement et apporter de la valeur aux consommateurs, les OC doivent collecter des données personnelles sur leurs utilisateurs et leur environnement. Or, les consommateurs sont de plus en plus réticents à les communiquer car ils éprouvent des craintes quant à l'utilisation et au devenir de ces données. Ces craintes sont en partie fondées car les entreprises qui commercialisent des OC ont parfois des difficultés à s'autoréguler sur les questions de vie privée et de confidentialité (Acquisti et al., 2020). En réponse, les consommateurs établissent des « frontières informationnelles » qui définissent comment, avec qui et dans quelle mesure ils divulguent leurs informations personnelles (*« privacy circles »* (Jagadish, 2020)). Parallèlement, les autorités régulatrices tentent de protéger les utilisateurs au travers d'initiatives telles que le RGPD (Règlement Général sur la Protection des Données) en Europe ou le CCPA (*California Consumer Privacy Act*) en Californie. Ces politiques publiques ont certes amélioré les pratiques des entreprises mais force est de constater qu'il subsiste encore des zones d'ombre. La façon dont les données sont collectées et utilisées demeure opaque et peu transparente du point de vue des consommateurs, créant une situation d'asymétrie d'information qui rend leurs choix complexes. Prenant appui sur la théorie du signal (Spence, 1973), nous nous interrogeons sur les leviers dont disposent les consommateurs pour réduire l'asymétrie d'information et limiter leur vulnérabilité et les préoccupations liées à leur vie privée dans un contexte d'achat d'OC (ici une enceinte connectée). Selon cette théorie, les consommateurs peuvent s'appuyer sur un ensemble de signaux de nature interne (émis par les entreprises) ou externe (émis par des entités tierces) afin de pallier l'asymétrie d'information (Bergen et al., 1992). Devant la propagation des signaux proposés aux consommateurs (marque, prix mais aussi labels externes) il semble difficile d'identifier leur réel impact sur la décision d'achat. L'interaction de ces signaux devient alors un enjeu et questionne sur la façon dont le consommateur opère dans ses choix. En appliquant la théorie du signal à un contexte d'asymétrie d'information sur la gestion des données personnelles nous proposons dans cette recherche de tester l'effet d'un signal (interne et externe) mais également l'effet d'interaction entre eux. Dans cette recherche, nous proposons de tester l'impact d'un signal externe (le *privacy score*), qui prend la forme d'un étiquetage indicatif du respect de la vie privée, sur la préoccupation pour la vie privée des consommateurs, leur vulnérabilité perçue et leur intention d'achat d'un OC. Nous étudions également l'effet simultané d'un signal interne (la marque) et d'une variable individuelle (l'expertise technologique perçue).

Littérature et hypothèses de recherche

Préoccupation pour la vie privée et vulnérabilité perçue

La gestion des données personnelles collectées par les OC constitue une situation d'asymétrie forte entre entreprises et consommateurs. Les politiques de confidentialité des entreprises qui proposent des OC sont souvent complexes, opaques, voire intentionnellement floues. Les consommateurs éprouvent alors de réelles difficultés à les juger, à évaluer les fabricants et à choisir un produit. Cela se traduit par des évaluations et des sentiments négatifs qui peuvent modeler les intentions et comportements. La préoccupation pour la vie privée (*privacy concern*) et la vulnérabilité perçue constituent deux variables centrales dans l'explication des intentions et comportements des consommateurs (Martin et al., 2017).

La préoccupation pour la vie privée. Depuis maintenant de nombreuses années, le marketing se heurte aux préoccupations des consommateurs quant à l'utilisation et la divulgation de leurs données personnelles (Caudill et Murphy, 2000). Divers travaux s'intéressent à ce phénomène (Westin, 1967 ; Sheehan et Hoy, 1999 ; Turow et al., 2009 ;

Goldfarb et Tucker, 2011 ; Martin et al., 2017). La préoccupation pour la vie privée représente une variable très souvent explicative de la formation des attitudes négatives des consommateurs à l'égard de la marque. Miltgen et al. (2016) appréhendent la préoccupation pour la vie privée comme une perception d'un risque par le consommateur lié à la collecte, l'utilisation, la diffusion et à la combinaison de ses données afin de reconstruire une identité permettant de lui proposer des offres commerciales au plus proches de ses centres d'intérêts. La plupart des recherches sur la préoccupation pour la vie privée considère le concept comme un trait de personnalité. Dans cette recherche, nous l'appréhendons comme une variable situationnelle, de nature cognitive, à l'image de Lwin et al. (2007). Nous étudions ici le rôle médiateur de la préoccupation pour la vie privée entre les signaux perçus par les consommateurs et leur intention d'achat d'une enceinte connectée. Sheehan et Hoy (1999) indiquent que lorsque la préoccupation pour la vie privée augmente, les comportements négatifs des individus augmentent et inversement. Aussi, nous posons l'hypothèse suivante :
H1 : La préoccupation pour la vie privée a un effet négatif sur l'intention d'achat d'un OC.

La vulnérabilité perçue. Martin et al. (2017) définissent la vulnérabilité perçue comme le sentiment lié à l'utilisation des données personnelles du point de vue du consommateur. Lorsqu'une entreprise recueille, stocke et utilise les informations personnelles de ses clients, elle crée un préjudice potentiel et, par conséquent, crée un sentiment de vulnérabilité (Martin et al., 2017). Même lorsque le dommage réel subi par le consommateur est mineur, cela augmente de manière significative ce sentiment de vulnérabilité perçue (Solove, 2003). La vulnérabilité perçue implique des effets négatifs tels que l'anxiété perçue et un sentiment de violation potentielle, de trahison, de colère (Martin et al., 2017). Afin de réduire cette perception de vulnérabilité, les consommateurs limitent les informations sensibles qu'ils partagent et s'impliquent parfois même dans un processus de réactance (Acquisti et al., 2020). Comparativement à la préoccupation pour la vie privée, la vulnérabilité perçue est de nature plus affective et devrait être négativement liée à l'intention d'achat.
H2 : La vulnérabilité perçue a un effet négatif sur l'intention d'achat d'un OC.

La théorie du signal

La théorie du signal suggère que les entreprises comme les consommateurs utilisent des signaux pour faire face aux situations d'asymétrie d'information (Nelson, 1970 ; Tellis et Wernerfelt, 1987 ; Erdem et Swait, 1998 ; Kirmani et Rao, 2000). Les signaux sont des messages diffusés intentionnellement ou non, que les destinataires observent et décodent dans le but de réduire une asymétrie d'information (Boulding et Kirmani, 1993 ; Kirmani et Rao, 2000 ; Connelly et al., 2011). Les signaux communiquent des informations sur des éléments qui ne sont pas directement observables tels que la qualité d'un produit et les risques associés (Rao et al., 1999). Ils sont qualifiés d'internes lorsqu'ils sont contrôlés par le marketing (ex : la marque, le prix ou une publicité) ou d'externes lorsqu'ils ne sont pas contrôlables par le marketing (ex : une information proposée par une entité tierce) (Akdeniz et al., 2014). Si les deux types de signaux atténuent l'asymétrie d'information, leur influence diffère et est sujette à des effets d'interaction (substitution ou complémentarité) (Akdeniz et al., 2014).

Le rôle d'un signal externe : effet du privacy score. Le *privacy score* que nous introduisons ici est un système d'étiquetage propre au respect de la vie privée. A l'image du Nutri-score, il prend la forme d'un logo synthétique d'information permettant au consommateur d'estimer le niveau de risque relatif à la collecte, la gestion et la diffusion de ses données personnelles lors de l'achat d'un OC. Le *privacy score* constituerait un signal externe, un levier de transparence informant les consommateurs sur les risques dans la collecte et l'utilisation des données liés à l'achat et à l'usage d'un OC (Ho et al., 2009 ; Treiblmaier et Pollach, 2007 ; Portes et al., 2020). Il rendrait les informations plus lisibles et davantage intelligibles et représenterait également un élément d'objectivité puisque proposé

par une entité tierce. Le *privacy score* serait ainsi un moyen de signaler sa transparence, de limiter l'asymétrie d'information et de surmonter les risques relatifs à la divulgation des données personnelles.

H3a : Un privacy score vert (rouge) a pour effet de réduire (renforcer) la préoccupation pour la vie privée.
H3b : Un privacy score vert (rouge) a pour effet de réduire (renforcer) la vulnérabilité perçue.
H3c : Un privacy score vert (rouge) a pour effet de renforcer (réduire) l'intention d'achat d'un OC.

Le rôle d'un signal interne : effet de la marque. Parmi l'ensemble des signaux potentiels, la marque peut constituer un signal de marché crédible pour informer les consommateurs et réduire la situation d'information imparfaite (Erdem et Swait, 1998 ; 2004). « Une marque devient un signal car elle incarne (ou symbolise) les stratégies marketing passées et présentes d'une firme » (Erdem et Swait, 1998, p. 135-136). La marque peut ainsi apparaitre comme un signal permettant de réduire les coûts d'acquisition d'informations ainsi que le risque perçu associé à un achat. Elle est donc source d'utilité pour le consommateur car elle lui procure des informations précieuses pour faire face à l'incertitude caractéristique des situations d'asymétrie informationnelle (Erdem et Swait, 1998 ; 2004 ; de Chernatony et Riley, 1999 ; An et al., 2019 ; Rao et al., 1999). Néanmoins, cet effet ne peut opérer que si la marque est crédible ce qui implique que le consommateur la perçoive comme ayant la capacité (expertise) et la volonté (bienveillance) de respecter durablement ses engagements » (Erdem et Swait, 2004, p. 192)[1]. En revanche, Le modèle de suspicion défensive développé par Darke et Ritchie (2007) explique que les jugements de suspicion à l'égard d'une marque impliquent des comportements défensifs et d'autoprotection.

H4a : Une marque crédible (non-crédible) a pour effet de réduire (renforcer) la préoccupation pour la vie privée.
H4b : Une marque crédible (non-crédible) a pour effet de réduire (renforcer) la vulnérabilité perçue.
H4c : Une marque crédible (non-crédible) a pour effet de renforcer (réduire) l'intention d'achat d'un OC.

Effets d'interaction entre le privacy score et la marque. Lorsque plusieurs signaux sont simultanément présents, leurs effets dépendent les uns des autres (Akdeniz et al., 2014). Selon Akdeniz et al. (2014), les consommateurs sont susceptibles de percevoir comme plus crédible la présence simultanée de signaux de natures différentes (interne et externe). La transmission simultanée de deux signaux dissemblables se traduit par un effet de complémentarité en augmentant l'efficacité de chacun d'entre eux. Inversement, la présence de deux signaux semblables peut réduire l'efficacité individuelle de chacun d'entre eux. La crédibilité d'un signal est alors affaiblie lorsqu'il est accompagné d'un signal de nature similaire ; il y a donc un effet de substitution (Maheswaran et Chaiken, 1991). Ainsi, nous proposons que la marque (signal interne) et le *privacy score* (signal externe) opèrent selon une logique de complémentarité. Le signal externe (le *privacy score*), perçu comme plus crédible, serait renforcé par un signal interne (la marque) lorsque celui-ci est perçu positivement.

H5 : L'effet du privacy score sur l'intention d'achat d'un OC est modéré par la marque.
H5a : L'effet positif d'un privacy score vert sera plus important pour une marque avec un fort niveau de crédibilité que pour une marque avec un faible niveau de crédibilité.
H5b : L'effet négatif d'un privacy score rouge sera plus faible pour une marque avec un fort niveau de crédibilité que pour une marque avec un faible niveau de crédibilité.

La prise en compte des variables individuelles : l'effet de l'expertise technologique perçue

Si les signaux dont dispose le consommateur peuvent en partie expliquer ses attitudes et comportements, des caractéristiques personnelles peuvent modeler leurs effets. Nous nous intéressons ici à l'expertise technologique perçue comme facteur limitant la perception de

[1]Ces deux composantes (expertise et bienveillance) rappellent les éléments centraux constitutifs de la confiance. Aussi, dans cette recherche, le terme crédibilité doit être entendu au sens de Erdem et Swait (2004) et ne pas être confondu avec la notion de crédibilité utilisée en marketing et constituant une dimension de la confiance.

risques à l'égard de l'environnement digital. Plus précisément, nous nous centrons sur l'expertise perçue par rapport à l'utilisation des OC qui représente la « capacité à accomplir des tâches liées au produit. Elle repose sur les structures cognitives (par exemple, les perceptions des attributs d'un produit) ainsi que sur les processus cognitifs (par exemple, les prises de décisions fondées sur ces perceptions) requis pour accomplir ces tâches » (Alba et Hutchinson, 1987). Cette variable est positionnée comme un modérateur de l'effet du *privacy score* sur les attitudes et intentions d'achat. Lorsqu'un consommateur est peu familier dans une catégorie de produit, les signaux utilisés pour réaliser des inférences lui sont essentiels (Kirmani et Rao, 2000) ; il aura tendance à y être plus attentif qu'un consommateur expert qui perçoit moins de risques et de vulnérabilité quant à sa vie privée (Portes et al., 2020). Aussi, nous proposons les hypothèses suivantes :

H6 : L'effet du privacy score est modéré par l'expertise technologique perçue.

H6a : L'effet du privacy score sur la préoccupation pour la vie privée sera réduit (renforcé) lorsque le niveau d'expertise est fort (faible).

H6b : L'effet du privacy score sur la vulnérabilité perçue sera réduit (renforcé) lorsque le niveau d'expertise est fort (faible).

H6c : L'effet du privacy score sur l'intention d'achat d'un OC sera réduit (renforcé) lorsque le niveau d'expertise est fort (faible).

Méthodologie de la recherche

Design et stimuli expérimentaux. Cette étude manipule 2 facteurs en mode intersujets : le *privacy score* (Vert *vs.* Rouge) et la marque (Apple *vs.* Xiaomi). Les stimuli représentent une fiche produit d'une enceinte connectée comme l'on pourrait en trouver sur n'importe quel site e-commerce (cf. annexe 2). Le format du *privacy score* s'inspire des logos synthétiques d'information déjà implantés sur le marché (étiquettes de performance énergétique ou de qualité nutritionnelle comme le Nutri-score). Ces derniers sont faciles à identifier et permettent de prendre des décisions plus rapidement et avec moins d'efforts que les logos analytiques (Ducrot et al., 2015 ; Julia et Hercberg, 2017). Ils sont également plus efficaces pour classer les produits sur le critère de qualité retenu (Ducrot et al., 2015) et permettent de mieux alerter sur la faible qualité et de promouvoir la forte qualité des produits sur ce critère (Mérigot et Nabec, 2016).

Participants et procédure. 268 répondants représentatifs de la population française ont été aléatoirement assignés à l'une des 4 conditions expérimentales. Ils devaient s'imaginer en situation d'achat d'une enceinte connectée. Après avoir pris connaissance de la marque de l'enceinte, ils devaient évaluer leur degré de confiance vis-à-vis de cette marque. Puis, une explication du *privacy score* était donnée. Enfin, s'affichait la page de présentation de l'enceinte. Les dernières questions portaient sur l'identification des répondants. Les variables étaient mesurées par des échelles de Likert en 7 points (1 = pas du tout d'accord ; 7 = tout à fait d'accord). L'annexe 3 présente l'ensemble des items retenus.

Vérification de la manipulation. Des ANOVA[2] montrent que le *privacy score* influence significativement le niveau de préoccupation pour la vie privée qui est plus élevé lorsque le *privacy score* est rouge (M_{rouge} = 5,75) que lorsqu'il est vert (M_{vert} = 5,37). Il influence également le niveau de vulnérabilité perçue (F = 23,88 ; p < 0,01) qui est plus élevé lorsque le

[2]Un prétest a tout d'abord été réalisé sur un échantillon de 134 personnes. Il a permis de confirmer, grâce à des ANOVA, l'effet des variables manipulées. Ainsi, le *privacy score* vert (M_{vert} = 4,82) génère un niveau d'intrusion perçue moins élevé que le rouge (M_{rouge} = 5,45) (F = 8,60 ; p < 0,01). Quant aux marques, Apple (M_{Apple} = 4,70) obtient un score de confiance plus élevé que Xiaomi (M_{xiaomi} = 4,10) (F = 8,12 ; p < 0,01). En outre, les stimuli utilisés ne présentent pas de différences significatives en termes de crédibilité et de réalisme du scénario (p > 0,10).

privacy score est rouge (M_{rouge} = 5,32) que lorsqu'il est vert (M_{vert} = 4,45). Enfin, le *privacy score* influence significativement l'intention d'achat (F = 19,46 ; p < 0,01) qui est plus élevée lorsque le *privacy score* est vert (M_{vert} = 3,32) que lorsqu'il est rouge (M_{rouge} = 2,35).

Estimation du modèle et résultats

Le modèle (cf. annexe 1) a été testé grâce à la macro PROCESS[3] (Hayes, 2013). Les résultats montrent que la préoccupation pour la vie privée (B = -0,18 ; p < 0,05) et la vulnérabilité perçue (B = -0,45 ; p < 0,01) ont un impact négatif sur l'intention d'achat, corroborant H1 et H2. Un *privacy score* favorable a pour effet de réduire la vulnérabilité perçue (B = -0,80 ; p < 0,01) et de renforcer l'intention d'achat (B = 0,98 ; p < 0,01), supportant H3b et H3c. Néanmoins, il n'a pas d'effet sur la préoccupation pour la vie privée (B = -0,27 ; p > 0,10), infirmant H3a. La marque a un effet direct positif sur l'intention d'achat (B = 0,53 ; p < 0,05), corroborant H4c, mais n'influence ni la préoccupation pour la vie privée (B = -0,04 ; p > 0,10) ni la vulnérabilité perçue (B = -0,06 ; p > 0,10), infirmant H4a et H4b. Conformément à H5, la marque modère la relation entre le *privacy score* et l'intention d'achat (a x b = -0,92 ; p < 0,05). Les résultats montrent ainsi que l'intention d'achat est significativement affectée par le *privacy score* mais seulement lorsque le niveau de crédibilité de la marque est faible (cf. annexe 5). Le *privacy score* n'a pas d'effet lorsque la marque est jugée crédible. Marque et *privacy score* entretiennent donc une relation de substitution et non de complémentarité, infirmant H5. Concernant l'expertise technologique perçue, son effet modérateur n'est pas vérifié, infirmant H6. Néanmoins, l'expertise technologique perçue a un impact direct négatif sur la préoccupation pour la vie privée (B = -0,27 ; p < 0,05) ainsi que sur la vulnérabilité perçue (B = -0,28 ; p < 0,01) et un impact positif sur l'intention d'achat (B = 0,26 ; p < 0,05).

Discussion et implications

Implications théoriques. Ce travail montre que les signaux agissent tout d'abord de manière individuelle. Ainsi, la marque comme le *privacy score* influencent directement l'intention d'achat. En outre, l'étude de leur interaction suggère un effet de substitution (et non de complémentarité), la marque se substituant au *privacy score* lorsque celle-ci est perçue comme crédible. Ainsi, la crédibilité dans la marque aurait pour effet de gommer les effets du *privacy score* sur l'intention d'achat. Ces résultats sont en partie concordants avec les travaux sur le Nutri-score (Nabec et al., 2019) qui suggèrent que son effet est modéré par le type de marque (MDD *vs.* marque nationale). Mais ils sont contradictoires avec les travaux antérieurs qui montrent que les signaux externes sont plus crédibles et donc plus efficaces que les signaux internes et qu'ils tendent ainsi à s'y substituer lorsque les deux sont présents (Albrecht, 1981 ; Akdeniz et al., 2014). Il apparait donc que la présence simultanée des signaux internes et externes n'est pas nécessairement favorable à ces derniers et que la nature intrinsèque des signaux doit également être considérée. Néanmoins il convient de reconnaitre que la marque n'influence pas directement les attitudes. Elle n'a d'effet que sur l'intention d'achat et n'est pas de nature à modeler les préoccupations pour la vie privée ou les sentiments de vulnérabilité contrairement au *privacy score*. Les résultats montrent aussi que le *privacy score* agit de manière indirecte sur l'intention d'achat mais seulement au travers de la vulnérabilité perçue. Il n'influence pas la préoccupation pour la vie privée. L'effet indirect du *privacy score* emprunte donc une voie plus affective que cognitive en influençant les sentiments de vulnérabilité chez le consommateur et non les risques perçus de violation de sa vie privée. Enfin, l'expertise technologique perçue agit non pas comme un modérateur des

[3]Modèle 10 avec 5000 bootstraps. Les variables continues incluses dans les termes d'interaction ont été transformées à plus ou moins un écart-type.

effets du *privacy score* mais comme un antécédent direct des attitudes et de l'intention d'achat. Le *privacy score* est un élément d'information utile pour réaliser une décision d'achat, que l'on se perçoive comme expert ou non des OC.

Implications managériales. Cette recherche montre que les marques caractérisées par une faible confiance de la part des consommateurs devraient d'abord miser sur la mise en place d'une politique de confidentialité irréprochable afin d'obtenir des labels de respect de la vie privée, tels que le *privacy score*. Cela ne doit cependant pas les freiner dans le déploiement d'investissements marketing dédiés à la création d'une marque forte puisque celle-ci peut se substituer au *privacy score*, dès lors qu'elle est jugée crédible aux yeux des consommateurs. Étant donné la présence toujours plus grande des OC, l'affichage d'informations sur le respect de la vie privée des consommateurs par les entreprises peut devenir un levier de différenciation et d'expression du positionnement de leurs marques. Par ailleurs, dans une perspective de marketing social, rendre obligatoire l'affichage du *privacy score* permettrait d'orienter les choix de consommateurs vers des produits plus respectueux de leur vie privée et inciterait les entreprises à mener une vraie réflexion sur leur politique de confidentialité.

Limites et voies de recherche. Cette recherche présente certaines limites. Tout d'abord, le *privacy score* n'existe pas réellement même si les pouvoirs publics réfléchissent à la mise en place d'une certification des plateformes numériques destinée au grand public (JO n°53 du 4 mars 2022) et qu'au sein d'un projet de recherche interdisciplinaire des juristes et des informaticiens travaillent sur l'élaboration de ce score. En outre, la manipulation proposée ici n'intègre pas de groupe de contrôle et ne permet ainsi pas de comprendre pleinement les effets de la présence (*vs.* l'absence) du *privacy score*, qu'il soit favorable ou défavorable. Par ailleurs, les marques choisies dans notre expérimentation ne sont pas neutres et présentent de fortes disparités en termes de notoriété, d'image et de communication de leur politique de confidentialité. Il serait opportun de réaliser une autre étude en neutralisant par exemple les effets liés à la marque. Finalement, nous pouvons nous demander quelle est la véritable compréhension du signal (le *privacy score*) par l'utilisateur et la crédibilité qu'il peut lui accorder ?

Références

Acquisti A, Brandimarte L et Loewenstein G. (2020) Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology 30*(4) : 736-758.

Akdeniz MB, Calantone RJ et Voorhees CM (2014) Signaling quality: an examination of the effects of marketing□and nonmarketing□controlled signals on perceptions of automotive brand quality. *Journal of Product Innovation Management 31*(4) : 728-743.

Alba JW et Hutchinson JW (1987) Dimensions of consumer expertise. *Journal of Consumer Research* 13(4) : 411-454.

An J, Do DKX, Ngo LV et Quan THM (2019) Turning brand credibility into positive word-of-mouth: integrating the signaling and social identity perspectives. *Journal of Brand Management 26*(2) : 157-175.

Bergen M, Dutta S et Walker Jr OC (1992) Agency relationships in marketing: A review of the implications and applications of agency and related theories. *Journal of Marketing 56*(3) : 1-24.

Boulding W et Kirmani A (1993) A consumer-side experimental examination of signaling theory: do consumers perceive warranties as signals of quality?. *Journal of Consumer Research 20*(1) : 111-123.

Caudill EM. et Murphy PE (2000) Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing* 19(1) : 7-19.

Connelly BL, Certo ST, Ireland RD et Reutzel, CR (2011) Signaling theory: A review and assessment. *Journal of Management* 37(1) : 39-67.

Darke PR et Ritchie RJ (2007) The defensive consumer: Advertising deception, defensive processing, and distrust. *Journal of Marketing Research* 44(1) : 114-127.

De Chernatony L et Riley FDO (1999) Experts' views about defining services brands and the principles of services branding. *Journal of Business Research 46*(2) : 181-192.

Ducrot P, Méjean C, Julia C, Kesse-Guyot E, Touvier M, Fezeu L, Hercberg S et Péneau S (2015) Effectiveness of front-of-pack nutrition labels in French adults: Results from the NutriNet-Santé cohort study. *PLoS ONE* 10(10) e0140898.

Erdem T et Swait J (1998) Brand equity as a signaling phenomenon. *Journal of Consumer Psychology 7*(2) : 131-157.

Erdem T et Swait J (2004) Brand credibility, brand consideration, and choice. *Journal of Consumer Research 31*(1) : 191-198.

Flynn LR et Goldsmith RE (1999) A short, reliable measure of subjective knowledge. *Journal of Business Research 46*(1) : 57-66.

Goldfarb A et Tucker C, (2011) Privacy regulation and online advertising. *Management Science* 57(1) : 57-71.Hayes A (2013) *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach.* New York: Guilford Press.

Ho A, Maiga A et Aimeur E (2009) Privacy protection issues in social networking sites. *2009 IEEE/ACS International Conference on Computer Systems and Applications* : 271-278.

Jagadish H V (2020) Circles of privacy. *Journal of Consumer Psychology* 30(4) : 774-779.

Julia C et Hercberg S (2017) Development of a new front-of-pack nutrition label in France: The 5-colour Nutri-Score. *Public Health Panorama* 3(4) : 712-25.

Kirmani A et Rao AR (2000) No pain, no gain: A critical review of the literature on signaling unobservable product quality. *Journal of Marketing 64*(2) : 66-79.

Lwin M, Wirtz J et Williams JD (2007) Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science 35*(4) : 572-585.

Maheswaran D et Chaiken S (1991) Promoting systematic processing in low-motivation settings: Effect of incongruent information on processing and judgment. *Journal of Personality and Social Psychology* 61 (1): 13–25.

Malhotra N, Kim S et Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15(4) : 336-355.

Martin KD, Borah A et Palmatier RW (2017) Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81(1) : 36-58.

Mérigot P et Nabec L (2016) Les effets d'alerte et de promotion des logos nutritionnels sur la face-avant des produits agroalimentaires. *Décisions Marketing* 83 : 29-47.

Lancelot Miltgen C, Henseler J, Gelhard C et Popovic A (2016) Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research* (69)10 : 4659-4666.

Nabec L, Marette S. et Durieux F. (2019), Les effets du Nutri-Score en France sur le consentement-à-payer des consommateurs à faible revenu, *Décisions Marketing*, 96, 69-88.

Nelson P (1970) Information and consumer behavior. *Journal of Political Economy* 78 (2): 311–29.

Portes A, N'Goala G et Cases AS (2020) La transparence numérique : dimensions, antécédents et conséquences sur la qualité des relations clients. *Recherche et Applications en Marketing* 35(4) : 73-102.

Rao AR, Qu L et Ruekert RW (1999) Signaling unobservable product quality through a brand ally. *Journal of Marketing Research 36*(2) : 258-268.

Sheehan KB et Hoy MG (1999) Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising 28*(3) : 37-51.

Solove DJ (2003) Identity theft, privacy, and the architecture of vulnerability. *Hastings Law Journal* 54 (1227) : 1–47.

Spence M (1973) Job market signaling. *Quarterly Journal of Economics* 87(3) : 355–74.

Tellis GJ et Wernerfelt B (1987) Competitive price and quality under asymmetric information *Marketing Science* 6(3) : 240–53.

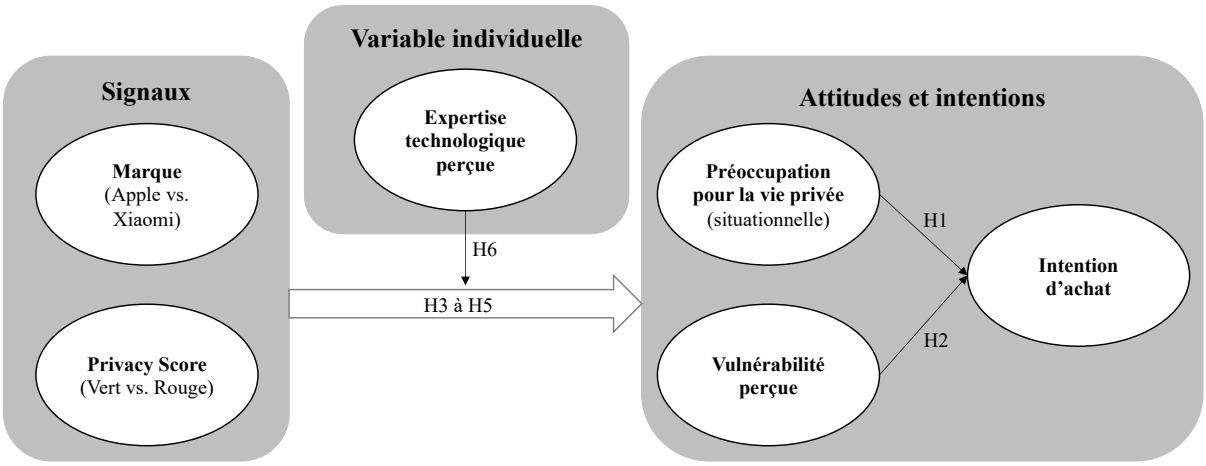
Treiblmaier H et Pollach I (2007) Users' perceptions of benefits and costs of personalization. *ICIS 2007 Proceedings* : 141.

Turow JM, King J, Hoofnagle C J, Bleakley A et Hennessy M (2009) Americans reject tailored advertising and three activities that enable it.

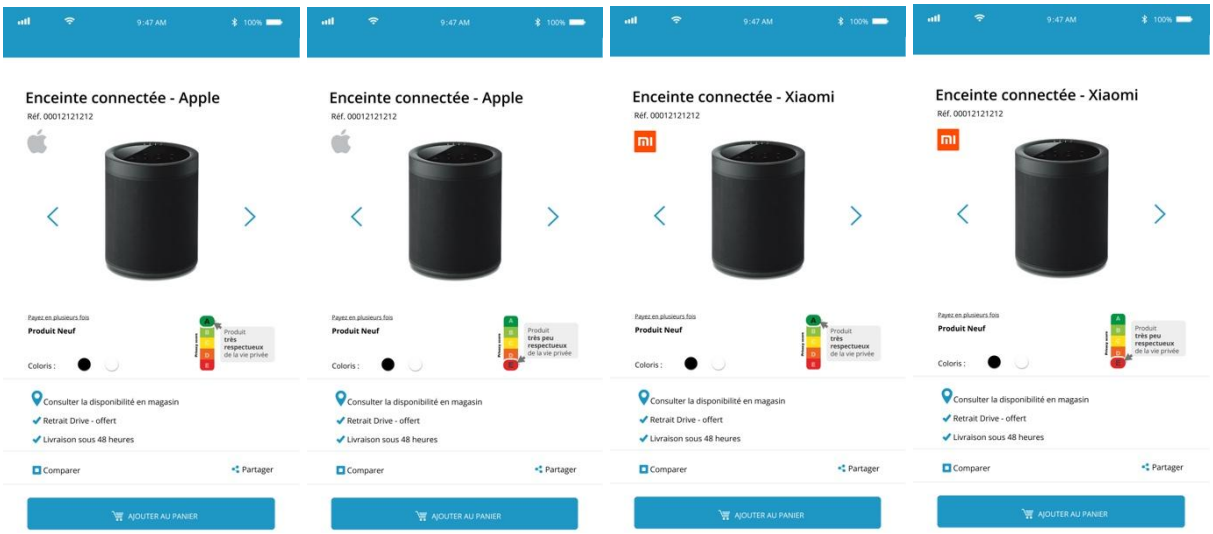
Westin AF (1967) Privacy and freedom. Atheneum, New York.

Annexes

Annexe 1 : Le modèle de recherche



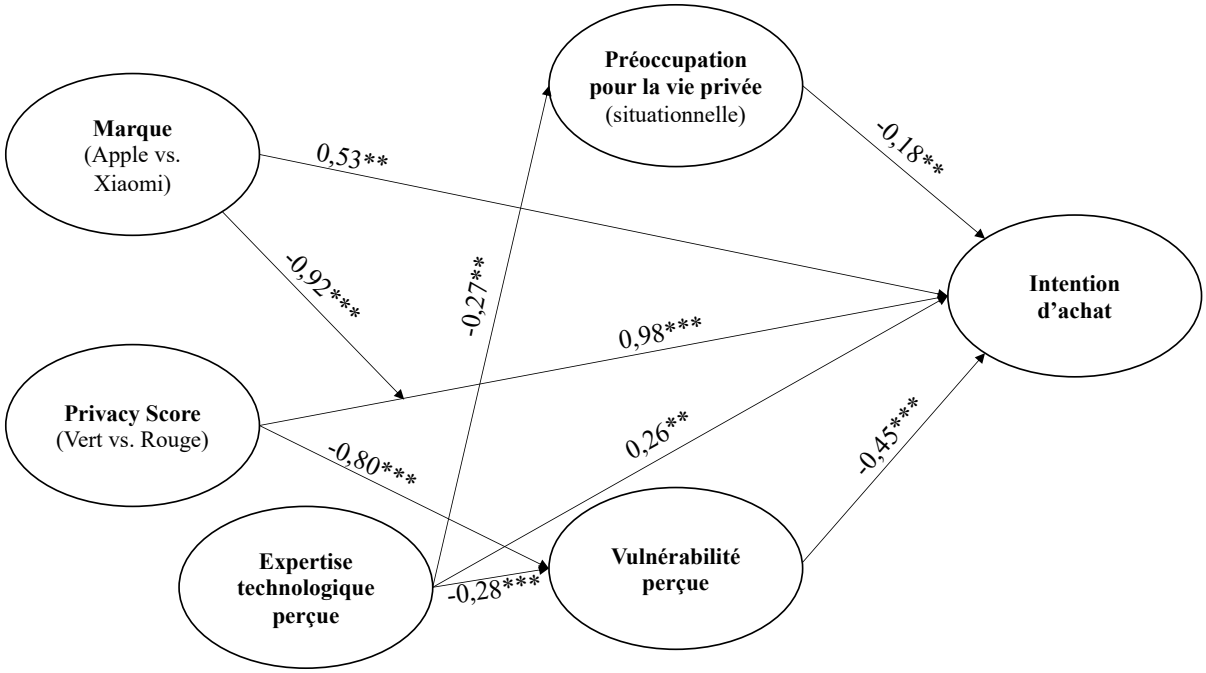
Annexe 2 : Les stimuli expérimentaux



Annexe 3 : Les échelles de mesure

Variables	**Items**
Expertise technologique perçue (Flynn et Goldsmith, 1999)	Je connais beaucoup de choses à propos des objets connectés
	Je ne me sens pas très bien informé vis-à-vis des objets connectés
	Parmi mes amis, je suis perçu comme un expert en objets connectés
	Comparé aux autres, je m'y connais moins en objets connectés
	A propos des objets connectés, je n'y connais vraiment pas grand-chose
Vulnérabilité perçue (Martin et al., 2017)	*Quant aux informations personnelles que la marque qui commercialise l'enceinte connectée pourrait collecter sur moi :*
	Je ne me sens pas en sécurité
	Je me sens exposé
	Je me sens menacé
	Je me sens vulnérable
	Je ne me sens pas à l'aise
Préoccupation pour la vie privée *(situationnelle)* (Lwin et al., 2007)	Dans quelle mesure craignez-vous que vos données personnelles soient utilisées à des fins autres que celles pour lesquelles vous les avez fournies lors de l'utilisation de l'enceinte connectée
	Dans quelle mesure êtes-vous préoccupé par le respect de votre vie privée lors de l'utilisation de l'enceinte connectée
	Dans quelle mesure êtes-vous préoccupé par le fait que la marque puisse savoir/suivre ce que vous faites lorsque vous utilisez l'enceinte connectée
	Dans quelle mesure êtes-vous préoccupé par le fait que la marque puisse partager à des tiers les informations collectées lors de l'utilisation de l'enceinte connectée
Confiance dans la marque (prétest) (Martin et al., 2017)	Je fais confiance à cette marque
	Cette marque est digne de confiance
	J'ai confiance dans la manière dont cette marque se comporte
	Cette marque est fiable
Intention d'achat (Malhotra et al., 2004)	*Compte-tenu du scenario d'achat proposé, seriez-vous prêt à acheter cette enceinte connectée ?*
	Improbable / Probable
	Invraisemblable / Vraisemblable
	Possible / Impossible *(item inversé)*
	Disposé / Réticent *(item inversé)*

Annexe 4 : Résultats de la recherche



Annexe 5 : le rôle modérateur de la marque