Pourquoi cette note?

Cette note rappelle l'urgence qui découle de la recommandation de la CNIL, qui s'applique à toutes les entreprises françaises ainsi qu'à toutes les organisations étrangères ciblant des citoyens français; Son but premier vise néanmoins à montrer concrètement comment la recherche en marketing permet de répondre aux défis qui découlent de cette annonce:

1. Pour mieux comprendre les mécanismes en comportements du consommateur en lien avec la collecte et l'utilisation des données par les entreprises (p. 2 à 6)
2. Pour concevoir l'email que toutes les entreprises françaises ou ciblant des consommateurs établis sur le territoire français doivent envoyer d'ici le 14 Juillet 2026 (p.6 à 7)
3. Pour proposer une étude (gratuite) visant à minimiser l'opt-out des clients (p.8 à 10)

Executive summary

Les pixels de suivi dans les emails permettent aux entreprises de collecter des informations telles que la date et l'heure d'ouverture d'un email, l'appareil utilisé et la géolocalisation approximative du destinataire.

À la suite de la recommandation de la CNIL, les entreprises doivent mettre à jour leurs processus et, à partir du 14 juillet 2026, recueillir des consentements distincts pour les communications par email et pour les pixels de suivi dans les emails. Pour les clients déjà présents dans leurs bases de données, un email d'information incluant un mécanisme d'opt-out du pixel de suivi doit être envoyé avant le 14 juillet 2026.

La volonté des consommateurs d'accorder leur consentement découle d'un arbitrage entre les coûts / risques perçus associés à la collecte de données et les bénéfices qu'ils s'attendent à recevoir en retour. La personnalisation représente l'un de ces bénéfices et, à condition d'être effectivement perçue comme ayant de la valeur, elle peut accroître la volonté des consommateurs de partager leurs données. Toutefois, les recherches antérieures suggèrent que la personnalisation peut également générer des effets contre-intuitifs selon le type de données utilisé, pouvant conduire à une résistance ou à un refus accru.

La recommandation de la CNIL rend visible une pratique de collecte de données qui était jusqu'à présent largement restée invisible pour les consommateurs. Par conséquent, les entreprises font face au risque d'une augmentation des taux d'opt-out, non seulement pour le consentement au pixel de suivi, mais aussi pour le canal email lui-même.

Envoyer simplement un email d'information centré sur la compliance n'est pas la solution optimale. Au-delà du respect des exigences réglementaires, les entreprises devraient également communiquer la valeur créée par la personnalisation afin d'atténuer les conséquences négatives potentielles.

En nous appuyant sur les avancées récentes de la littérature académique, nous proposons deux expériences de terrain : l'une conçue pour minimiser les taux d'opt-out au pixel de suivi parmi les clients existants, et l'autre visant à maximiser à la fois les taux d'opt-in à l'email et au pixel de suivi parmi les futurs clients.

Rappel du contexte de la recommandation de la CNIL

Le 14 avril, la CNIL a publié ses nouvelles lignes directrices sur les pixels de suivi dans les emails (utilisés pour suivre les ouvertures, les horodatages, la géolocalisation et l'appareil)[1]. La CNIL exige désormais un consentement préalable distinct pour le pixel de suivi, en plus du consentement à recevoir des emails pour les nouveaux clients:

Les entreprises ont jusqu'au 14 juillet 2026 pour se mettre en conformité, et doivent informer tous les clients contactables (email opt-in) de l'existence du pixel, de ce qu'il suit, et proposer une possibilité d'opt-out (sans qu'il soit nécessaire de recueillir à nouveau l'email opt-in)

Ainsi, pour de nombreux clients, cet email révélera l'existence d'une collecte de données « passive », c'est-à-dire l'existence de données collectées de manière discrète comme sous-produit des interactions quotidiennes des consommateurs avec une entreprise. (cf. Kraft et al., 2021; Kim et al., 2019).

→ **Il existe un risque qu'une large part des clients contactables refusent le pixel de suivi et que cet email génère en outre des désabonnements aux emails.**

À travers cette note et l'étude proposée, nous visons à répondre à deux questions :

1. Comment minimiser l'email opt-out parmi les clients qui découvrent l'existence de la collecte de données ?
2. Comment maximiser le consentement au pixel de suivi pour les nouveaux clients ?

Qu'est ce qui explique le refus des individus de partager leurs données aux entreprises ?

Le principal facteur découle de l'importance que les individus accordent à leurs données personnelles, capturée par le concept de préoccupations en matière de vie privée ("privacy concerns" en VO) (Malhotra et al., 2004; Smith et al., 2011): Celles et ceux qui sont extrêmement préoccupés par la vie privée forment des heuristiques de décision pour protéger leur vie privée et rejetteront probablement rapidement les demandes de données des entreprises. À l'inverse, ceux qui sont moins préoccupés par la vie privée n'auront probablement pas d'heuristique de protection de la vie privée et pourraient passer plus de temps à examiner les demandes de données.

Les individus valorisent leurs données personnelles et peuvent chercher à les protéger pour deux raisons distinctes : des raisons intrinsèques et instrumentales (Lin, 2022; Jerath et al., 2025). La vie privée intrinsèque renvoie à la valorisation de la vie privée pour elle-même. Dans ce cas, les individus

[1] https://www.cnil.fr/fr/recommandation-pixel-suivi-courriels

peuvent choisir de ne pas partager certaines données parce qu'ils les considèrent comme privées et ne souhaitent pas qu'une entreprise y ait accès. À l'inverse, et en pratique souvent de manière complémentaire, la vie privée instrumentale renvoie à la vie privée comme moyen d'éviter des conséquences négatives. Les individus protègent leurs données parce que leur divulgation pourrait être utilisée contre eux, par exemple au moyen d'une discrimination par les prix ou d'autres usages stratégiques défavorables. Alors que la vie privée intrinsèque peut être comprise comme une attitude relativement stable à l'égard des informations personnelles, la vie privée instrumentale dépend du contexte : par exemple, divulguer son poids à un médecin n'est pas perçu de la même manière que le divulguer à une application dont les serveurs sont basés en Chine ou aux USA.

La recherche s'accorde généralement à considérer que le refus ou l'acceptation du partage de données peut être expliqué comme le résultat d'une comparaison connue sous le nom de calcul de la vie privée ("privacy calculus" en VO) (équivalent à la vie privée instrumentale) : les individus comparent les bénéfices et les coûts associés au partage de données.

Beke et al., (2022) ont synthétisé plusieurs bénéfices et coûts. En ce qui concerne les bénéfices :

- les bénéfices financiers : soit par le biais d'incitations telles que des remises, des rabais ou des prix plus bas adaptés au profil du client ;
- les bénéfices de performance : l'offre ou les communications ultérieures sont personnalisées selon les préférences personnelles de l'individu, elles sont plus efficaces, et l'entreprise commet moins d'erreurs ;
- les bénéfices psychologiques : les données permettent une plus grande proximité avec l'entreprise, qui connaît mieux ses clients et peut mieux identifier ses meilleurs clients ;
- les bénéfices liés au temps : grâce à un meilleur ciblage par l'entreprise, les clients peuvent trouver plus rapidement les meilleurs produits.

Il est important de souligner des résultats contre-intuitifs et divergents concernant l'impact des bénéfices financiers sur le consentement : Kraft et al., (2017) ne trouvent aucun effet auprès d'un panel de répondants en Allemagne par rapport à d'autres bénéfices, tels que la personnalisation ; à l'inverse, D'assergio et al., (2025) identifient, à grande échelle, qu'une incitation monétaire dans le contexte du RGPD facilite le consentement. Koh et al., (2020) montrent dans le secteur des soins de la peau que les incitations fonctionnent, mais pas pour tous les clients : ce levier est plus efficace chez les clients plus jeunes que chez les clients plus âgés. En outre, le risque associé aux incitations est que, selon le type de client et son rapport aux données personnelles, l'argent puisse renforcer la valeur que les consommateurs attribuent à leurs données personnelles (Tomaino et al., 2023). En ce qui concerne les coûts, Beke et al., (2022) ont synthétisé six coûts/risques qui doivent être pris en compte afin de rassurer les consommateurs :

- Le risque lié à la performance est que l'utilisation des données ne bénéficie qu'à l'entreprise;
- Le risque financier est que l'utilisation des données puisse augmenter les prix;
- Le risque psychologique est lié à une perte de contrôle sur les données ou au sentiment d'être observé;
- Le risque social est lié à la possible divulgation des données et à la conséquence de devoir expliquer à leurs proches la raison pour laquelle les clients ont partagé leurs données;

- Le risque de sécurité concerne la question de savoir si les données sont transmises à d'autres entreprises, si elles pourraient être utilisées pour une usurpation d'identité, si elles sont publiques, et qui peut y accéder en interne;
- Le risque lié au temps concerne la question de savoir si les clients doivent passer du temps à remplir des formulaires, à protéger leur identité ou à surveiller la manière dont l'entreprise gère la protection des données.

Ainsi, la personnalisation peut produire des effets paradoxaux : alors que son impact positif sur le partage de données par les consommateurs a été établi (Schumann et al., 2014), elle peut générer de la réactance, c'est-à-dire un rejet par le consommateur lorsqu'elle devient apparente ("overt" en VO), lorsque le bénéfice n'est pas perçu par le consommateur, ou lorsqu'elle génère des préoccupations en matière de vie privée (Awad & Krishnan, 2006; Krafft et al., 2021; Lambillotte et al., 2022).

La méta-analyse d'Eisend et al., (2026) confirme ces effets paradoxaux en identifiant que les niveaux de personnalisation importent — la personnalisation faible à modérée constitue la pire zone, souvent perçue comme « creepy » et inconfortable, affaiblissant la persuasion, tandis que des niveaux élevés génèrent les résultats positifs les plus forts (achats, satisfaction, clics) et les réactions négatives les moins nombreuses. C'est pourquoi la personnalisation doit être utilisée avec prudence : la faire « un peu » peut se retourner davantage contre l'entreprise que ne pas la faire du tout.

Le type de données utilisées dans la personnalisation façonne également le résultat. L'utilisation de données implicites ("covert"/ "inferred" en VO) tend à éviter les préoccupations en matière de vie privée uniquement tant que les consommateurs n'en ont pas conscience — et seulement si les inférences sont exactes. En revanche, si les individus détectent que des données implicites sont utilisées, cela paraît plus intrusif et moins acceptable que des données explicitement fournies; et les inférences faites à partir des données qui se révèlent incorrectes amplifient le sentiment de violation de la vie privée. L'utilisation de données explicites ("overt" en VO), en revanche, renforce l'effet positif de la personnalisation lorsque les consommateurs les fournissent activement, mais la collecte explicite de données active la connaissance du client d'une tentative de persuasion, ce qui peut générer du rejet. Parce que ces mécanismes vont dans des directions opposées, les résultats nécessitent d'être étudiés au cas par cas, en distinguant les données "overt", "covert" / "implicites" plutôt qu'en traitant la « personnalisation » comme une tactique unique et uniforme.

Dans ce contexte, il est important de considérer la sensibilité perçue des données et, par conséquent, le risque potentiel perçu par les consommateurs si les données venaient à être divulguées (Acquisti et al., 2012; Mothersbaugh et al., 2012).

Le problème est que cette perception est subjective et varie donc selon les individus. Si certains types de données sont perçus comme plus sensibles, telles que les données financières, médicales et de géolocalisation (Phelps et al., 2001), d'autres sont perçus comme moins sensibles, telles que les données démographiques. Cependant, la sensibilité perçue des données de réactivité aux emails reste incertaine. Les données comparables qui s'en rapprochent le plus pourraient être les données de consommation média en ligne, que Grosso et al. (2020) considèrent comme modérément sensibles dans le secteur de la distribution. En outre, tandis que les données de contact (email) sont perçues comme très sensibles, les données comportementales en ligne sont perçues comme moins sensibles (Mothersbaugh et al., 2012).

Enfin, d'autres facteurs importants à prendre en compte incluent le volume de données collectées par l'entreprise (Martin et al., 2017) et le secteur d'activité : les secteurs qui traitent des données considérées comme sensibles, tels que la banque et l'assurance, font l'objet d'un examen plus attentif.

Il existe plusieurs profils de clients concernant la collecte, le stockage et l'utilisation des données par les entreprises.

Historiquement : la segmentation de la vie privée de Westin (Harris and Westin, 1998) classe les individus dans l'un de trois groupes : les « privacy fundamentalists », les « privacy pragmatists » et les « privacy unconcerned ». Plus récemment, Plangger & Montecchi, (2020) ont identifié quatre profils ayant des attentes très différentes concernant les données personnelles et les bénéfices à offrir. Pour trois catégories de consommateurs, le consentement au pixel de suivi semble concevable:

- Les "Unconcerned" : ils n'attendent pas de valeur et ne sont pas préoccupés par leurs données.
- Les "Capitalists" : « qui sont principalement motivés par la maximisation de la valeur fonctionnelle (par exemple, réduire le prix, obtenir une meilleure offre, accéder à des promotions), bien que les dimensions de valeur émotionnelle (par exemple, se sentir bien) et conditionnelle (par exemple, occasion spéciale) jouent également un rôle dans leur décision de divulguer [....] Pour les capitalists, les demandes de partage de données sont refusées non pour des raisons liées à la vie privée des consommateurs, mais en raison de l'absence d'utilité explicite ou de l'irritation suscitée par le manque de commodité. »
- Les "Pragmatists" : « pour qui les données personnelles sont vues comme des marchandises qui doivent être protégées et ne sont partagées qu'en échange de bénéfices précieux. » Le type de relation avec l'entreprise et les valeurs de l'entreprise entrent dans le calcul de la vie privée.

Dans le même temps, il existe également un segment de consommateurs pour lequel l'obtention du consentement sera plus difficile, voire impossible : les "Protectionists" sont « fortement préoccupés par la vie privée des consommateurs mais ne sont pas préoccupés par la valeur pour le consommateur. Ainsi, ils sont susceptibles de refuser rapidement les demandes de partage de données personnelles même lorsque des bénéfices précieux sont proposés, en raison du risque pour leurs données personnelles. Ces "protectionists" sont principalement préoccupés par la limitation des risques liés à leur vie privée [...].» La solution proposée par les auteurs est d'offrir davantage d'informations sur la manière dont leurs données personnelles sont collectées, stockées et utilisées, ainsi que fournir des garanties concernant la sécurité des données, afin d'atténuer certaines des préoccupations de ce segment de consommateurs.

Pallant et al., (2022) ont quantifié ces différents segments de clients : Indifferent (29.5% des consommateurs), Data Protectors (38.5% des consommateurs) et Exchange Advocates (32.1% des consommateurs).

Il convient également de noter qu'il existe une hétérogénéité entre les clients selon les variables socio-démographiques : les femmes partagent en général plus souvent leurs données (Aiello et al.,

2020; Krafft et al., 2017) ; mais selon le type de données, les hommes partagent parfois davantage (Grosso et al., 2020; Lin, 2022) ; et les individus plus jeunes partagent davantage leurs données que les individus plus âgés (Beke et al., 2022; Grosso et al., 2020).

Qu'est-ce qui affecte le consentement des individus à partager leurs données ?

Eggers et al., (2023) ont montré que ce ne sont pas seulement les bénéfices perçus par le client qui doivent être proportionnels aux données fournies ; la manière dont ces bénéfices sont communiqués importe également.

- Les consommateurs doivent donc être rassurés au sujet de la collecte des données, à savoir le type et le volume de données collectées, au sujet du stockage de ces données, et au sujet de l'utilisation de ces données, à savoir la personnalisation.
- Cela doit être fait de manière transparente, en ce qui concerne la collecte, le stockage et l'utilisation, tout en donnant aux consommateurs du contrôle afin de faciliter le consentement du consommateur. Toutefois la transparence est une arme à double tranchant However, these two dimensions are a "double edged sword": en effet, la transparence, qui est requise par la CNIL, peut rendre les consommateurs conscients des pratiques de collecte de données et amplifier les préoccupations en matière de vie privée, tout comme le contrôle, requis par la CNIL sous la forme d'un opt-out pour les clients existants et d'un opt-in pour les futurs opt-ins email à partir du 14/6/2026, peut réduire la quantité de données que l'entreprise peut collecter et utiliser.

Que révèle la recherche pour aider à formuler l'email devant être envoyé d'ici le 14 Juillet 2026 ?

La confiance est le mécanisme clé pour faciliter la propension à partager ses données personnelles (« willingness to share information » en VO) (Cloarec, 2020; Grosso et al., 2020). La confiance d'un client envers l'entreprise repose sur trois dimensions : la crédibilité perçue, c'est-à-dire l'évaluation de la capacité de l'entreprise à tenir ses promesses et à répondre aux attentes fonctionnelles, sur la base de l'expertise perçue ; l'intégrité, c'est-à-dire la perception de l'honnêteté de l'entreprise et du respect de ses promesses ; et la bienveillance, c'est-à-dire la perception que l'entreprise agit dans l'intérêt du consommateur, y compris au-delà de ses intérêts de court terme.

L'email « CNIL » est un moment de vérité pour construire la confiance. Deux éléments devront être fournis : alors que la CNIL exige que l'entreprise soit transparente et pédagogique concernant le pixel de suivi, les données collectées, leur(s) utilisation(s), et la mise à disposition d'une option d'opt-out, c'est également une opportunité, comme le notent Zeng et al., (2021), de fournir des réassurances concernant la protection des données et la déclaration de personnalisation.

- La réassurance en matière de vie privée aide les clients à évaluer plus précisément les risques pour la vie privée impliqués lorsqu'ils partagent des données personnelles aux

entreprises, en clarifiant la responsabilité des entreprises d'assurer la sécurité de leurs données → Cela correspond à la dimension d'intégrité.

- La déclaration de personnalisation implique les bénéfices futurs que les entreprises peuvent offrir aux clients → Cela correspond à la dimension de bienveillance

Nous proposons que la section relative à la personnalisation vise à « crédibiliser » la dimension de crédibilité en rendant visible une forme « invisible » de personnalisation, à savoir le nombre d'emails reçus et/ou ouverts (cf. partie suivante, p.8 et 9)

En analysant les demandes d'opt-in à la suite du RGPD, D'Assergio et al., (2024) révèlent qu'il existe trois stratégies possibles pour une demande de consentement :

1. une stratégie exclusivement informative où la communication détaille la manière dont les données personnelles sont collectées, traitées, et les actions que les utilisateurs peuvent entreprendre;
2. une stratégie exclusivement persuasive où la communication met en avant le caractère désirable de l'échange de données en fournissant des récompenses ou en le présentant comme bénéfique pour obtenir des avantages ou éviter des pertes potentielles associées au service ou au produit;
3. entre les deux, une stratégie mixte combinant information et persuasion.

→ La stratégie la moins efficace est celle fondée uniquement sur l'information, tandis que la stratégie fondée uniquement sur la persuasion n'est pas compatible avec la recommandation de la CNIL. Une stratégie mixte devrait donc être adoptée : information + mise en avant des bénéfices.

Concernant le CTA : Romero et al., (2026) ont montré qu'il est préférable d'utiliser des termes fondés sur la reconnaissance ou la prise de conscience, par exemple « Je suis informé » ou « Je comprends », plutôt que des termes fondés sur une autorisation explicite, par exemple « Autoriser » ou « Accepter ». Si le vocabulaire fondé sur la permission est perçu comme plus direct, il rend le risque pour la vie privée plus saillant et réduit la volonté de consentir.

Il convient de noter que cet effet est plus prononcé dans les secteurs du quotidien / à faible risque, tels que la distribution ou le divertissement ; il n'existe pas de différence dans les secteurs bancaire ou de la santé entre les formulations. Chez les clients qui ne sont pas préoccupés par leur vie privée, la formulation n'a pas d'impact, contrairement aux clients qui sont plus préoccupés.

Proposition de recherche

La participation à ce projet est gratuite. Nous proposons de conduire les analyses et traduirons les résultats en recommandations pour votre entreprise.

De notre point de vue, l'objectif principal est de produire des connaissances académiques à travers la publication des résultats. Afin de protéger la confidentialité, les données ainsi que l'identité de votre organisation peuvent être anonymisées, sans problème et sur demande.

Sans vouloir verser dans le sensationnalisme, les implications pour votre entreprises sont importantes : dans la mesure où la recommandation de la CNIL s'applique à toutes les entreprises ciblant des consommateurs français, les campagnes emailing qui seront envoyées au cours des prochaines semaines sont susceptibles d'accroître plus largement les préoccupations en matière de vie privée et la réactance des consommateurs. Par conséquent, vos clients pourraient non seulement refuser le consentement au pixel de suivi, mais également saisir cette occasion pour se désabonner totalement des communications par email.

Une vague massive d'opt-outs au pixel de suivi aurait des conséquences majeures pour la mesure de l'email marketing. Sans consentement au pixel de suivi, les entreprises ne pourront plus suivre les ouvertures d'emails, rendant obsolètes les reportings actuels. Les KPIs traditionnels tels que les taux d'ouverture et les taux de réactivité ne seraient plus fiables pour trois raisons : la mesure de l'ouverture deviendrait incomplète, car elle exclurait à la fois les nouveaux clients qui n'accordent pas leur consentement au pixel de suivi et les clients existants qui exercent leur opt-out. Plus important encore, la mesure deviendrait systématiquement biaisée, dans la mesure où les clients fournissant à la fois le consentement à l'email et au pixel de suivi sont généralement les clients les plus engagés (i.e fort biais de sélection). Et, à terme, cela rendrait les comparaisons historiques entre campagnes de plus en plus difficiles, voire impossibles.

Par conséquent, nous vous proposons 2 expériences de terrain afin d'adresser ces problématiques

Emailing d'information sur le pixel de suivi à envoyer d'ici le 14 Juillet 2026 - A/B test du type de personnalisation employée

Comme discuté précédemment, il est essentiel de démontrer les bénéfices concrets de la personnalisation. La recommandation de la CNIL rend visible une pratique de collecte de données qui était jusqu'à présent largement restée invisible pour les consommateurs. Nous proposons donc de tirer parti de cette exigence de transparence pour illustrer directement, dans l'email lui-même, la valeur générée par ces données.

Cela conduit à notre question de recherche : quels types de données de personnalisation utilisées dans les emailings sont les plus efficaces pour minimiser les taux d'opt-out au pixel de suivi ?

	Information uniquement (controle)	Personnalisation #1 Données de l'entreprise	Personnalisation #2 Données du client
Randomisation	Bénéfice de la personnalisation utilisé comme élément de persuasion : "Les données d'ouverture nous permettront d'ajuster la fréquence et le contenu des emails que vous recevez"	Bénéfice montré avec les données de l'entreprise : "Vous avez reçu n emails en 2026 ; n concernaient cette catégorie de produits, et n concernaient une autre catégorie de produits. En utilisant vos données d'ouverture, nous serons en mesure d'ajuster la fréquence et le contenu des emails en fonction du contenu que vous préférez"	Bénéfice montré avec les données de réactivité du client : "Vous avez ouvert y emails, et nous prenons cette information en compte pour ajuster la fréquence et le contenu des emails en fonction du contenu que vous préférez"

Au-delà de l'estimation des effets causaux des interventions proposées, il serait utile de caractériser les profils des clients qui consentent à l'utilisation du pixel de suivi par rapport à ceux qui exercent leur opt-out. L'exploitation des données CRM (par exemple, données socio-démographiques, ancienneté de la relation, valeur client et réactivité passée aux emails) nous permettrait d'identifier des différences systématiques entre ces groupes. Ces enseignements pourraient aider les entreprises à anticiper quels segments de clients sont les plus susceptibles de refuser de futures formes de collecte de données, notamment dans la mesure où la CNIL entend étendre cette exigence de consentement préalable aux liens de tracking dans les emailings..

Mettre à jour vos processus de collecte des double opt-ins à partir du 14 Juillet 2026

L'obtention de deux opt-ins distincts crée un point de friction supplémentaire dans le parcours client et peut donc augmenter les taux de refus. La recherche en psychologie sociale a depuis longtemps documenté l'effet de pied-dans-la-porte ("foot-in-the-door effect" en VO chez Freedman & Fraser, 1966 par exemple), selon lequel l'acceptation d'une première demande peut accroître la probabilité d'accepter une demande ultérieure.

Bien que la séquence des demandes soit elle-même largement contrainte dans notre contexte (le consentement email doit logiquement précéder toute demande par email de consentement au pixel de suivi), deux dimensions de design restent ouvertes à l'expérimentation :

- Le canal par lequel le consentement au pixel de suivi est demandé ;
- Le cadrage (“framing” en VO) utilisé pour présenter la demande de consentement.

Ces deux facteurs devraient influencer la volonté des clients de fournir leur consentement à l’email et au pixel de suivi.

En conséquence, nous proposons une expérience de terrain randomisée afin d’identifier le design de demande de consentement qui maximise les taux de double opt-in :

Randomisation # 1	**Opt-ins simultanés (même canal)**	**Opt-ins séquentiels (même canal)**	**Opt-ins séquentiels (canaux différents)**
	Les deux opt-ins (email & pixel) sur la même page du site web	- Opt-in email sur une page du site web - Opt-in pixel sur une page différente du site web	- Opt-in email sur une page du site web - Opt-in pixel dans un emailing dédié
Randomisation # 2	**Cadrage neutre**	**Cadrage par les bénéfices**	**Cadrage par les coûts**
	Informatif uniquement	Valeur offerte au client en accordant son opt-in	Comment réduire le coût perçu du partage de données, c’est-à-dire les garanties relatives aux données

Ce que nous devons garantir pour cette expérience :

1. Le cadrage doit être maintenu constant (within-subject design) entre les demandes d’opt-in (par exemple, même cadrage par les bénéfices pour les opt-ins email & pixel)
2. Que la randomisation fonctionne, en comparant si les différents bras de traitement sont équilibrés sur les covariables pré-traitement. Grâce aux session IDs et aux cookies, nous devrions pouvoir observer le type d’appareil (mobile/desktop), la source de trafic (organic/paid/social), la géolocalisation approximative basée sur l’adresse IP (pays/région), le pourcentage de nouveaux visiteurs, le nombre de pages vues avant la manipulation.

Des questions ?

Contacts

Tom VILLENET (Doctorant @iaelyon School of Management)
tom.villenet2@univ-lyon3.fr

Klaus MILLER (Maître de conférences @HEC)
Titulaire de la chaire de recherche Hi! Paris Center for AI and Data Science
millerk@hec.fr

William SABADIE (Professeur des Universités @iaelyon School of Management)
Responsable scientifique de la chaire de recherche Lyon3 Coopération
william.sabadie@univ-lyon3.fr

Bibliography

Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V., & Viglia, G. (2020). Customers' Willingness to Disclose Personal Information throughout the Customer Purchase. *Journal of Retailing*, *96*(4), 490‑506. https://doi.org/10.1016/j.jretai.2020.07.001

Awad, N. F., & Krishnan, M. S. (s. d.). *The Personalization Privacy Paradox : An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization1*. Consulté 26 mai 2026, à l'adresse https://dx.doi.org/10.2307/25148715

Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2022). Consumers' privacy calculus : The PRICAL index development and validation. *International Journal of Research in Marketing*, *39*(1), 20‑41. https://doi.org/10.1016/j.ijresmar.2021.05.005

Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change*, *161*, 120299. https://doi.org/10.1016/j.techfore.2020.120299

D'Assergio, C., Manchanda, P., Montaguti, E., & Valentini, S. (2024). The Race for Data : Utilizing Informative or Persuasive Cues to Gain Opt-In? *Journal of Marketing*, https://doi.org/10.1177/00222429241288456

Eggers, F., Beke, F. T., Verhoef, P. C., & Wieringa, J. E. (2023). The Market for Privacy : Understanding How Consumers Trade Off Privacy Practices. *Journal of Interactive Marketing*, *58*(4), 341‑360. https://doi.org/10.1177/10949968221140061

Eisend, M., Niewiadomska, D., & van Noort, G. (2026). EXPRESS : Personalization in Marketing Communication: A Meta-Analysis. *Journal of Marketing*, https://doi.org/10.1177/00222429261460888

Freedman, J. L., & Fraser, S. C. (1966). Compliance without pressure : The foot-in-the-door technique. *Journal of Personality and Social Psychology*, *4*(2), 195‑202. https://doi.org/10.1037/h0023552

Grosso, M., Castaldo, S., Li, H. (Ariel), & Larivière, B. (2020). What Information Do Shoppers Share? The Effect of Personnel-, Retailer-, and Country-Trust on Willingness to Share Information. *Journal of Retailing*, *96*(4), 524‑547. https://doi.org/10.1016/j.jretai.2020.08.002

Jerath, K., Miller, K. M., & Sokol, D. D. (2025). *Towards Developing an Understanding of Consumers' Perceived Privacy Violations in Online Advertising* (arXiv:2403.03612). arXiv. https://doi.org/10.48550/arXiv.2403.03612

Kim, T., Barasz, K., & John, L. K. (2019). Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness. *Journal of Consumer Research*, *45*(5), 906‑932. https://doi.org/10.1093/jcr/ucy039

Koh, B., Raghunathan, S., & Nault, B. R. (2020). An empirical examination of voluntary profiling : Privacy and quid pro quo. *Decision Support Systems*, *132*, 113285. https://doi.org/10.1016/j.dss.2020.113285

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission Marketing and Privacy Concerns—Why Do Customers (Not) Grant Permissions? *Journal of Interactive Marketing*, *39*(1), 39‑54. https://doi.org/10.1016/j.intmar.2017.03.001

Krafft, M., Kumar, V., Harmeling, C., Singh, S., Zhu, T., Chen, J., Duncan, T., Fortin, W., & Rosa, E. (2021). Insight is power : Understanding the terms of the consumer-firm data exchange. *Journal of Retailing, Re-Strategizing Retailing in a Technology Based Era*, *97*(1), 133‑149. https://doi.org/10.1016/j.jretai.2020.11.001

Lambillotte, L., Bart, Y., & Poncin, I. (2022). When Does Information Transparency Reduce Downside of Personalization? Role of Need for Cognition and Perceived Control. *Journal of Interactive Marketing*, *57*(3), 393‑420. https://doi.org/10.1177/10949968221095557

Lin, T. (2022). Valuing Intrinsic and Instrumental Preferences for Privacy. *Marketing Science*, *41*(4), 663‑681. https://doi.org/10.1287/mksc.2022.1368

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC) : The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336‑355.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context : The Role of Sensitivity of Information. *Journal of Service Research*, *15*(1), 76‑98. https://doi.org/10.1177/1094670511424924

Pallant, J. I., Pallant, J. L., Sands, S. J., Ferraro, C. R., & Afifi, E. (2022). When and how consumers are willing to exchange data with retailers : An exploratory segmentation. *Journal of Retailing and Consumer Services*, *64*, 102774. https://doi.org/10.1016/j.jretconser.2021.102774

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns : An empirical investigation. *Journal of Interactive Marketing*, *15*(4), 2‑17. https://doi.org/10.1002/dir.1019

Plangger, K., & Montecchi, M. (2020). Thinking beyond Privacy Calculus : Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, *50*(1), 32‑44. https://doi.org/10.1016/j.intmar.2019.10.004

Romero, M., Slejko, G., & Abell, A. (2026). The power of words : How linguistic framing affects consent in retail privacy policies. *Journal of Retailing*, *102*(1), 149‑164. https://doi.org/10.1016/j.jretai.2025.09.001

Schumann, J. H., von Wangenheim, F., & Groene, N. (2014). Targeted Online Advertising : Using Reciprocity Appeals to Increase Acceptance among Users of Free Web Services. *Journal of Marketing*, *78*(1), 59‑75. https://doi.org/10.1509/jm.11.0316

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research : An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989‑1015. https://doi.org/10.2307/41409970

Tomaino, G., Wertenbroch, K., & Walters, D. J. (2023). Intransitivity of Consumer Preferences for Privacy. *Journal of Marketing Research*, *60*(3), 489‑507. https://doi.org/10.1177/00222437221122994

Zeng, F., Ye, Q., Li, J., & Yang, Z. (2021). Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research*, *124*, 667‑675. https://doi.org/10.1016/j.jbusres.2020.02.006