Comments of the World Privacy Forum

To
The United States Postal Service

Regarding
A new system of records for the Informed Delivery Notification Service, 81 Federal Register 58542

Via FedEx and email

Chief Privacy Officer
USPS
475 L'Enfant Plaza SW
Room 1P830
Washington DC 20260
privacy@usps.gov

September 16, 2016

The World Privacy Forum welcomes the opportunity to comment on the US Postal Service's Privacy Act notice establishing a new system of records for the Informed Delivery Notification Service. The proposal appeared at 81 Federal Register 58542 on August 25, 2016, https://federalregister.gov/a/2016-20189.

The World Privacy Forum is a non-profit public interest research and consumer education group. We publish in-depth research papers, policy comments, and consumer education focusing on privacy and security issues. Much of our work explores emerging technology and privacy issues, including health, biometrics, consent, data analytics, and many other rapidly evolving areas of privacy. You can see our publications and more information at www.worldprivacyforum.org.

I. General Comments about the USPS Informed Delivery Notification Service SORN

A. Support for the SORN and background

First, we support the decision to establish a dedicated system of records for the Informed Delivery Notification Service (hereafter Informed Delivery).[1] Informed Delivery provides postal service customers with images of the front of letters and other envelopes that are scheduled to be delivered that day. Customers can see the scanned images of the outside of their mail on a mobile app.[2] The system is currently being tested in a handful of pilot locations and will expand to all zip codes in early 2017. [3] When the system goes nationwide it will also include images of catalogs and packages.[4] The Postmaster General described the Informed Delivery system as follows: "It gives every marketer the opportunity to attach a digital offer to mail pieces, and eventually packages. This is an incredibly powerful product for this industry."[5]

The Informed Delivery system is an important enough system to provide notice for the public, and a separate system of records increases transparency in a useful way. We support the decision to provide a notice for this system. However, we regret to say that there are serious deficiencies with this notice. We urge the USPS to publish a new notice containing additional information and to seek comments from the public again before making the system of records notice final. We include our detailed concerns in Section II of these comments.

B. General issues relating to ambiguity of the SORN

Second, regarding the content of the SORN, the most significant general question raised by the SORN is if the Informed Delivery System is going to be another surveillance system that allows USPS -- or others -- to track what users do in highly granular detail. The SORN is hazy and ambiguous on this point, and one of our general comments is that the SORN is not at all clear to us what data USPS intends to collect and how it will be used. The SORN does state that the information can be used for debt collection and given to credit reporting agencies, but the SORN is not clear on the other sharing involved with Informed Delivery.

For example, the SORN tells customers that the data collected from the Informed Delivery service will be used "to guide policy and business decisions through the use of analytics." This is obscure. Who are the other third parties here? Whose business decisions?

USPS needs to explain in more detail what personal or other customer data will be collected, how the data will be linked with other data, and how USPS or a marketing company will "determine the outcomes" of campaigns, how long that data will be kept, and what other government entities might have access to it, and for what purposes. We raise additional specific

---

[1] The Informed Delivery system is described as follows from the States News Service: "The Postal Service has also launched a pilot 'informed delivery' program, which sends customers emails with images and details about their letter and package mail before it's delivered that day, free of charge. Customers can then let the Postal Service know if they'd like the mail delivered to them." States News Service, *International Postal Update for April 2016*, 29 March 2016.

[2] See USPS Informed Delivery page http://realmail.usps.com/box/pages/intro/start.action.

[3] Tim Echols, *Meet the post office of the future*, Atlanta Business Chronicle, 21 March 2016.

[4] Al Urbanski, *PMG Brennan hails the dawning of a digital age at the Postal Service*, DM News, March 2016.

[5] Comments of Megan J. Brennan, US Postmaster General at the 2016 National Postal Forum, USPS press release (Globe Newswire), 21 March 2016.

questions in Section II of these comments, but in general, our concerns center around this chief issue and the multiple corollary questions it raises.

C. Difficulty of commenting via paper methods, and request for electronic submission options in the future

Third, we would like to mention a procedural issue. The USPS has made it difficult for the public to comment on this important new system of records. This SORN specifies either postal or hand delivery of comments. There was no electronic submission option offered. This meant that we had to print out our comments on paper and send them via FedEx to meet the deadline due to federal mail security requirements. As the USPS knows, all postal mail is X-rayed prior to delivery to federal addresses, and this can delay mail by as long as two weeks. For submitting comments with a short deadline, these delivery requirements were a burden.

It is a rarity to submit comments on paper to the US government these days. Nearly every government agency accepts electronic submission of public comments. At the very least, the USPS should provide clear and specific electronic submission options for commenting on the SORN. For example, an email address specified for electronic submission, or a way of commenting via the Federal Rulemaking Portal. We think it would be appropriate for the Postal Service to accept electronic as well as mailed comments on its future Privacy Act notices.

We note that after discussion, USPS agreed to accept this comment electronically. We appreciate the gesture, but that does not solve the problem that others face in commenting on the system notice.

We have additional specific questions and comments on the published notice, below.

II. Specific Comments about the SORN

A. Issues and questions about the Interactive Content

In the section describing the Rationale for the system, we find this statement:

> "Providing advance notice of mail delivery also allows consumers to take action before important pieces reach their mailbox, revolutionizing the customer experience with mail. In some cases, email notifications with mailpiece images will include interactive content, such as **"ride-along" images or related links from the business mailer**."[6] [emphasis ours]

We request clarification on what the bolded language means, as it is unclear. Here are the questions we have about this:

- Will there be a *click here* link or QR code that takes the recipient of a USPS message directly from the image of their mail to a third party website? This is an extremely

[6] 81 Federal Register 58542, pp. 58542-58544, https://www.federalregister.gov/articles/2016/08/25/2016-20189/privacy-act-of-1974-system-of-records.

important point for public understanding and should not be glossed over in the SORN. We note that USPS employees have described Informed Delivery as providing *click here* links directly from images of postal mail to marketing websites. We do not object to marketing. We do object to obscure language to describe the data controls around marketing for postal mail.[7]

- Will USPS track if and/or when users read Informed Delivery email? If so, is the tracking aggregate? Is it by name or device ID? Does the tracking tie to a specific address? How is the tracking done, and how long is that data stored? Who gets to see that data? Do third parties outside USPS, for example, get to see that data? Who gets to see if a piece of mail was seen at a specific physical address? Because customers are verified, this becomes an especially important point.
- It appears to us that a user of Informed Delivery will look at the email message with images of the user's postal mail and, along with the image, receive additional marketing messages or materials in some cases. Is this so?
- Will USPS track whether and when users read Informed Delivery email? Who or what businesses get that information?
- Is Informed Delivery going to be another surveillance system that allows USPS to track what users do and share the information with third parties?
- Additionally, the description of "interactive content" is incomplete and unclear. We request more information on what this means, and clarification on what this will be, specifically.
- Will information sent by one mailer be shared through Informed Delivery with another mailer?
- Will the USPS privacy policy be available directly on the Informed Delivery app? Will the notice disclose all tracking and third party sharing clearly?

The consequences of postal service customers using Informed Delivery need to be carefully explained to users. Users should be given an express choice about whether they are tracked and whether USPS can share any of their information with third parties when they use this system. We understand that this system is voluntary at this time. But the convenience of Informed Delivery should not be tied to its tracking features without giving users a choice about tracking. Why not build a system that allows USPS customers the ability to use this system and the ability to choose whether a third party can track certain of their mail choices? The SORN needs to explain the tracking and whether and/or why it is necessary or mandatory for the SORN to operate.

B. Will Informed Delivery create Informed Phishing?

[7] Al Urbanski, *Postal Service Debuts Digital Mail in New York*, Direct Marketing News, 23 November, 2015: "[USPS] VP of Innovation and New Products Gary Reblin said that a group of business mailers were recruited for the New York test. "If a direct mailer wants to give us an HTML, then we can actually make that piece click through to their website, so it can create a buy-it-now experience. So not only would the end mailer get more impressions, but they also create the easy capability to be able to click through and purchase," Reblin said in a *Direct Marketing News* podcast earlier this year."

We see Informed Delivery as potentially opening up fresh new opportunities for criminals, phishers, and spammers. News articles have noted that trials of the system allow for marketers to attach *click here* links to images of mailed letters. These links are said to deliver users **directly** to a marketing website.[8] While we understand the impetus here, and do not object to marketing, we would like to raise serious concerns about how customers could be deeply impacted by altogether new and better forms of phishing based on this new US Postal Mail Informed Delivery system.

There is already a considerable amount of email from fraudsters announcing fake package deliveries. The existing types of fake delivery emails are typically click bait to attract visitors, to collect personal information for nefarious uses, or in some cases to install malware. As soon as the Postal Service starts to deliver widespread scans of actual postal mail with *click here* links, we anticipate fraud problems to occur, including copycat USPS Informed Delivery emails that look identical but that will place those who *click here* in harm's way.

We understand that Informed Delivery is going to be mediated via an app. However, fraudulent emails can be sent to non-customers and be made to look very real. We have quite a few concerns about this issue, given the sophistication of today's phishers. No longer mom and pop operations, phishing emails today can look identical to official emails. There is no reason to believe images of postal mail with *click here* links cannot be made to look identical to Social Security checks and other common pieces of mail.

We do not object to email from USPS for those who want it, but creating a new opportunity in an environment where the crooks are already active and flourishing puts everyone in some danger, including those who did not sign up for Informed Delivery. We strongly recommend that USPS never allow any click-through links or other interactive content in email that it sends to Informed Delivery recipients. If this type of immediate "click through and buy" is allowed, much thought will need to be given to avoid a future phishing disaster. At the very least, there needs to be much more informed public discussion of this issue with core public groups working with vulnerable populations and financial fraud and privacy issues.

We also object, with a somewhat lesser degree of intensity, to the use of Informed Delivery email as another vehicle for spam. We recognize the Postal Service's need for revenue, but any contribution from new advertising revenue from this medium will be a drop in the ocean. It will not outweigh the strong objections that Americans have to spam. At the very least, each customer should be able to use the service and receive additional marketing messages only with affirmative consent of the customer.

C. Questions About Informed Delivery users

In a given household, there may be residents who receive postal mail though a common delivery funnel, whether that be a single mailbox attached to a home, or a cluster box at a dorm or apartment, or a nursing home or other group living facility. What about mail delivered to businesses, corporations, and government agencies? In general, it is up to the residents to determine what happens to the mail after delivery. Which of the residents will have the ability to

[8] Id at 6.

sign up for Informed Delivery? Will one customer per household be able to enroll? Will all customers in the household be able to enroll? Will customers who are not adults be able to enroll? Will adults be able to block children from enrolling? What safeguards are in place so children cannot be inadvertently targeted?

We foresee the possibility that Informed Delivery may exacerbate existing internal household conflicts over mail and over information about mail. In households where couples separate, Informed Delivery may allow one individual to keep track of activities of the other. We see these possibilities as important complexities in the program that require resolution, and we suggest that it may call for some more attention by USPS than the SORN currently reflects.

Additionally, we respectfully urge the USPS to consult with groups focusing on elders and other vulnerable members of society to proactively prevent unintended harms. We foresee potential safety issues related to victims of domestic violence and stalking as well as other violent crimes, and we foresee issues related to the privacy of health information coming by way of postal mail.

For example, if a person gets a bill from an alcohol or drug rehab unit, or a bill from a cancer center – there needs to be specific guidelines around the plethora of sensitive issues that will arise in this new system. Much will depend on how sign-up for the system is managed, and much will depend on how PII, click-throughs, and third party feedback on customer activity is managed.

D. Unclear definition of Customer Account Preferences

The SORN states a definition of customer account preferences as follows:

> "2. Customer account preferences: Individual customer preferences related to email and online communication participation level for USPS and marketing information."[9]

The reference to marketing information is unclear. What is the source and nature of the marketing information? Nothing in the description of records in the system explains what marketing information will be collected and maintained. Is the marketing information for USPS or for another entity? We don't know. The description here needs much clear and more granular, identifying each possible category of marketing information and recipient. If USPS plans to collect marketing information for mailers, that activity needs a much fuller explanation.

E. Lack of clarity regarding definition of Personally Identifiable Information

The SORN states a definition of personally identifiable information as follows:

> "7. User Data associated with 11-digit ZIP Codes: Information related to the user's interaction with Informed Delivery email messages, including, but not limited to email

[9] 81 Federal Register 58542, pp. 58542-58544, https://www.federalregister.gov/articles/2016/08/25/2016-20189/privacy-act-of-1974-system-of-records.

> open and click-through rates, dates, times, and open rates appended to mailpiece images (user data is not associated with personally identifiable information)."[10]

We are confused about the parenthetical stating "user data is not associated with personally identifiable information." An 11-digit ZIP Code is an identifier. It is associated with an address. If that address is a residential address and there is a single occupant, the 11-digit ZIP Code is uniquely associated with that occupant. Even if there are several residents at the address, the number is associated with only a few individuals and must be treated as the equivalent of an individual identifier.[11]

We do not understand how USPS can claim that an individual's interaction with Informed Delivery associated with an 11-digit ZIP Code does not create personally identifiable information. Certainly USPS knows who the individual is who enrolled in Informed Delivery. If USPS discloses information about that user, it cannot contend that the information is not personally identifiable. If USPS does contend this, it needs to state how this is so.

Even if only the machine interaction data plus the 11-digit zip is used, it is still going to be PII if MAC addresses and other identifying transactional data can be directly or indirectly collected and linked. We note for the record that USPS discloses on its current Informed Delivery privacy policy for the pilot program that email addresses are linked to physical addresses for pilot participants.[12] This is another PII linkage that requires careful thought.

F. Questions about Stated Purposes

The notice states that the USPS Informed Delivery system will collect data analytics, and describes this as follows:

> "USPS will also collect data analytics from mail campaigns sent through Informed Delivery in order to determine the outcomes of each campaign and help guide business decisions."[13]

Similarly, the SORN describes one of the purposes of the system as follows:

> "5. To determine the outcomes of marketing or advertising campaigns and to guide policy and business decisions through the use of analytics." [14]

---

[10] Id at 9.

[11] See for example, an early New York Times piece from 1998 discussing the modern and increasingly digitizing USPS network, and its precision in knowing its customer and being able to communicate customer actions to third parties: http://www.nytimes.com/1998/10/22/technology/it-may-be-snail-mail-but-technology-gets-it-where-it-s-going.html.

[12] The USPS Informed Delivery Privacy Notice introduction states: "To provide you with these images, Informed Delivery™ will need to link your physical mailing address with your email address that you have submitted through your usps.com® account." Accessed September 14, 2016. <http://realmail.usps.com/box/pages/intro/privacy.jsp>.

[13] Id at 9.

[14] Id at 9.

We discussed this issue in Section I of these comments. Again, it is not at all clear to us exactly what data USPS intends to collect and how it will be used. Telling customers that the data will be used "to guide policy and business decisions through the use of analytics" is inappropriately non-transparent. USPS needs to explain in more detail what personal or other data will be collected, how the data will be linked with other data, and how USPS or a marketing will "determine the outcomes" of campaigns.

We cannot, from this language, determine specifically how users of the system will be tracked through their mail, email, or other activities. The hint that there will be additional surveillance of Informed Delivery users is a significant concern, and we wonder how much surveillance is hidden in an obscurely written notice.

For example, will USPS track and inform marketers if a customer makes a purchase, has a later delivery, or sends an order or inquiry through snail mail or email?

G. Issues around retention and disposal

Regarding retention of data and personally identifiable information, the notice states:

> "Mailpiece images will be retained up to 7 days (mailpiece images are not associated with personally identifiable information)."[15]

We do not understand how an image of an item of postal mail delivered by email to an individual living at a specific address is not personally identifiable information. We recognize that some mail may not include either a name or an address, but the majority of mail contains both and thus constitutes personally identifiable information. If USPS can sort images and determine which image should be sent to a specific Informed Delivery user, it is apparent that there must be personally identifiable information associated with something. Admittedly, images kept only for seven days are a lesser concern, but the lack of clarity of the notice around PII remains at issue.

H. Questions about verification of postal customers

The notice says that customers "successfully complete one of several available verification processes." There is no detail or specification of the nature of the verification or the entities that USPS may use for the purpose.

We do not object to verifying the identity of users through the usual methods, but we cannot tell what USPS intends. We know that many verification procedures require either a Social Security Number match challenge, or a public records answer challenge. Simply put, verifying individual identity requires information about that individual. We do not know if the USPS plans to use social media accounts for identification or verification. If so, this introduces additional complexities to consider and account for in the SORN.

[15] Id at 9.

I. Objection to inclusion of Routine Use 10 that allows postal customer information to be given to debt collection agencies, credit risk assessment services, and credit bureaus

The inclusion of standard routine use 10 in the SORN is a problem because it is overbroad. Standard Routine Use 10 states:

> "10. Disclosure to Agencies and Entities for Financial Matters. Records may be disclosed to credit bureaus, government agencies, and service providers that perform identity verification and credit risk assessment services; to financial institutions or payees to facilitate or resolve issues with payment services; or to government or collection agencies for the purposes of debt collection or responding to challenges to such collection."[16]

We understand why enrollees in Informed Delivery must have their identities verified. We think that USPS should explain better how it plans to verify identities and the specific types of organizations that will undertake the verifications.

It is not clear whether or what identification verification USPS may obtain from a "government agency." Will USPS verify identities at the FBI, CIA, or NSA? We doubt it, but the breadth of the routine use allows it. The rest of the routine use that relates to payment services or debt collection seems completely irrelevant to Informed Delivery. We bet that most customers signing up for Informed Delivery have no idea that the verified information can be passed along to debt collectors and credit bureaus. We wonder if the information includes the email address linked to the physical address, and suspect this is the case. This is an issue that needs to be made clear if the RU 10 is kept, which we hope is not the case.

We suggest that instead of relying on standard routine use 10, USPS should add a narrowly tailored identity verification routine use to Informed Delivery and should not incorporate routine use 10 at all.

J. Objection to Routine Use 11, including the disclosure of Customer Records to multiple third parties, including mailers of sexually oriented advertisements

We also question the inclusion of routine use 11, which states that records may be disclosed to a broad variety of third parties.

> "11. Disclosure for Customer Service Purposes. Records may be disclosed to entities if the disclosure is part of the service to the customer. This includes disclosures to addressees of mail to process inquiries and claims; entities to which the customer wants to provide identity verification; the State Department for passport processing; international posts or agents to facilitate or process international services, claims, or inquiries; and mailers of sexually oriented advertisements to provide a list of customers who do not want to receive them."[17]

[16] Id at 9.
[17] Id at 9.

We are not sure what it means for a disclosure to be "part of the service to the customer." We cannot tell if any of the tracking or additional marketing that is part of Informed Delivery constitutes a service to the customer. At present, we cannot envision anything other than the email that a user receives as "part of the service to the customer." If that conclusion is correct, then there should be a simple and specific routine use that covers disclosures to email providers incident to sending an email message and that covers nothing else. We suggest that the reference to routine use 11 be dropped. It is overbroad.

In general, we observe that lumping too many routine uses in a single standard routine use allows for the possibility of disclosures that are not needed or compatible with a system's actual purpose. We suspect a review of other USPS SORNs would find similar issues. We cannot go back and change that history, but now that privacy knowledge, technology, and procedures have advanced significantly, USPS should revise its standard routine uses so that they are more granular.

Separate out each activity into its own routine use. We also suggest writing specific and narrow routine uses for specific Informed Delivery activities rather than relying on vague and unbounded standard routine uses. Finally, we much prefer that each system of records notice include the full text of all applicable routine uses rather than a reference to standard routine uses. Most if not all readers will have great difficulty finding the standard routine uses. It took us some effort to track down the Routine Uses, and we are familiar with how to do this.

III. Conclusion

The System of Record Notice for Informed Delivery lacks sufficient content and specificity to allow for a fair and complete evaluation. We urge the USPS to publish a new notice containing additional information and seek comment from the public again before making the system of records notice final. We believe the public will be very interested in this system after it becomes aware of the third party click-throughs tied to postal mail and linked to validated personal email addresses. This SORN has the potential to impact each US household receiving postal mail. It is important, and the public will eventually pay attention to it.

We hope future requests for public comment will specifically allow electronic submission of comments to encourage public feedback.

Thank you for the opportunity to comment on the Informed Delivery system of records notice. We would be pleased to answer any questions you may about our comments.

Respectfully submitted,

Pam Dixon
World Privacy Forum
www.worldprivacyforum.org