

A discussion of the two different aspects of privacy protection in indirect questioning designs

Andreas Quatember¹ 

Published online: 4 April 2018
© The Author(s) 2018

Abstract The motivation behind considering the use of indirect questioning designs is their possible positive effect on the respondents' willingness to cooperate. Whereas the privacy protection objectively offered by these methods has a direct effect on the estimator's efficiency, it is the subjectively perceived protection which affects the respondents' willingness to cooperate. For the discussion of these different aspects of privacy protection, a family of randomized response techniques enabling the tailoring of the design's privacy protection to the respondents is presented as representative of indirect questioning designs. Measures are suggested that formalize how the objectively offered and subjectively perceived privacy protection may differ. Different features of randomized response questioning designs, influencing the perceived privacy protection, are discussed particularly for the "crosswise model" in order to avoid underestimations of the true levels of privacy protection, which would be counter-productive with regard to the respondents' cooperation propensity.

Keywords Sensitive variables · Data confidentiality · Sampling theory · Survey methodology

1 Introduction

When questions on different sensitive subjects, such as income, voting behaviour, sexual orientation, alcoholism, drug usage, poverty, illegal employment, tax evasion, harassment at work, domestic violence, abortion, academic cheating, doping of amateurs and professionals, are asked in surveys using the usual direct-questioning method, the rates of

✉ Andreas Quatember
andreas.quatember@jku.at
<http://www.jku.at/ifas>

¹ Department of Applied Statistics, Johannes Kepler University JKU Linz, Altenberger Str. 69, 4040 Linz, Austria

nonresponse and untruthful answering might increase above the usual levels natural in survey sampling.

Let U be a finite universe of N population units and $s \subseteq U$ be a without-replacement probability sample of U consisting of $n \leq N$ elements drawn by a sampling method with knowable sample inclusion probabilities π_k ($k \in U$). Further, let A be a subgroup of U ($A \subseteq U$) and let variable $y_k = I\{k \in A\}$ indicate if a survey unit k is a member of A or not. The parameter of interest be the relative size

$$\pi_A = \frac{1}{N} \cdot \sum_U y_k \tag{1}$$

of A (\sum_U denotes the sum over the population units and \sum_s denotes the sum over the sample units). Moreover, let d_k be the design weight of population unit k , defined as usual as the reciprocal of π_k . Assuming full response and truthful answering, for general probability sampling, the proportion π_A from (1) is estimated by the unbiased Horvitz-Thompson (HT) based estimator

$$\pi_{A,HT} = \frac{1}{N} \cdot \sum_s d_k \cdot y_k \tag{2}$$

(cf., for instance, Särndal et al. 1992, p. 43ff). For the special case of simple random sampling without replacement (SI) with sample inclusion probabilities $\pi_k = n/N$ for all population units k , for example, the HT estimator (2) results in the mean of all y_k -values in the SI sample. The theoretical variance of $\pi_{A,HT}$ is given by

$$V(\pi_{A,HT}) = \frac{1}{N^2} \cdot \sum_U (\pi_{kl} - \pi_k \cdot \pi_l) \cdot \frac{y_k}{\pi_k} \cdot \frac{y_l}{\pi_l} \tag{3}$$

Therein, π_{kl} denotes the second-order inclusion probability that population units k and l of U are elements of s at the same time under the given probability sampling method. For SI sampling with $\pi_{kl} = \frac{n}{N} \cdot \frac{n-1}{N-1}$, Eq. (3) results in $\frac{\pi_A(1-\pi_A)}{n} \cdot \frac{N-n}{N-1}$.

However, when nonresponse and untruthful answers occur, like any other estimator the estimator $\pi_{A,HT}$ from (2) is affected by a decomposition of the sample set s into three non-overlapping, non-empty subsets: subset t consisting of all truthfully answering sampling units; subset u consisting of the untruthfully answering elements; and subset m consisting of the missing sampling units. Hence, such respondents' behaviour might cause serious problems because in subsets u and m of s the true values y_k cannot be observed. Weighting adjustment and data imputation are model-based statistical repair methods that try to compensate only for the occurred nonresponse after data collection (cf. for instance, Lohr 2010, ch. 8.5 and 8.6), but not for the untrue answers, which are held for the true answers. In contrast to these methods, indirect questioning designs such as the randomized response (RR) techniques discussed herein, or the item-count technique (cf. Chaudhuri and Christofides 2013), aim to address both problems at the same time before they actually occur. Hence, these methods can be seen as part of the system of preventative action with respect to nonresponse and untruthful answering, which includes so different things such as persuasion letters, data collection mode, interviewers' training or the offering of incentives (cf. Groves et al. 2004, Sec. 6.7).

In preparation for the comparison of objective and subjective protection of respondents' privacy in the subsequent sections, in Sect. 2 a family of RR techniques is presented as representative of indirect questioning designs extending its unified theory to allow tailored privacy protection on individual level. Section 3 measures of the objective level of privacy

protection provided by these RR strategies are presented and it is formally shown how this level affects the accuracy of the estimates. In Sect. 4, a formalization of the level of subjectively perceived protection of the respondents' privacy is considered. Furthermore, the impact of differing subjective and objective privacy protection on the interviewees' willingness to reply presuming a reasonably chosen level of objective privacy protection is discussed in particular for the crosswise model implementation of Warner's technique (1965) by Yu et al. (2008).

2 Randomized response questioning designs

A common characteristic of indirect questioning designs is that the actual process answer of any respondent cannot be directly linked to the sensitive variable under study. This fact should reduce the individual's fear of disclosure and thus, ensure respondents' cooperation by an increase of their perceived privacy protection.

For the discussion of the two different aspects of privacy protection following in Sects. 3 and 4, a certain family of RR techniques for the estimation of the relative size of population proportions of sensitive attributes according to (1) is presented as representative of all indirect questioning designs. The pioneering work in this field was done by Warner (1965): Following a certain randomization instruction, each respondent k has to answer randomly either with some probability $p_{1k} > 0$ the question 1: 'Are you a member of subgroup A of population U ?', or with the remaining probability p_{2k} the alternative question 2: 'Are you a member of the complementary subgroup A^C ?' ($A^C \subseteq U, A \cup A^C = U, A \cap A^C = \emptyset, 0 < p_{1k} \leq 1$). The needed randomization instruction can either be employed explicitly by a randomization device such as a coin, dice, deck of cards, or spinner or implicitly by a question unrelated to the sensitive subject with known answer distribution such as the question on the birth date or house number of some person. In the first case, the instruction may be, for instance, 'Throw a dice. If the dice is from 1 to 4, answer question 1, if not, question 2' or also the other way round because this RR design is "balanced" with respect to the protection of both possible answers. In the second case, the instruction may be 'Think of a person, whose date of birth you know. If the birth date is within the interval from 1st of January to 19th of October, answer question 1, if not, question 2' or the other way round. The use of such an implicit randomization instruction makes an RR design also suitable for self-administered data collection modes such as postal or online (cf. Höglinger and Diekmann 2017, p. 132).

In that paper, Warner also suggested an alternative implementation of the method (p. 68). The "contamination" approach (Boruch 1972, p. 404) instructs a respondent k with the probability p_{2k} to lie and with the probability p_{1k} to tell the truth about membership of group A . Although technically equivalent to the original design this approach might appear preferable from the "standpoint of increasing cooperation" (Warner 1965, p. 69).

An aspect of these two survey designs of Warner's technique is that the respondents will have to answer to the sensitive question, which psychologically might be problematic. Therefore, Yu et al. (2008) presented a less complex implementation of Warner's technique. In the "crosswise model", a respondent k is faced with two questions: Question 1 that can be seen as a disguise of the randomization instruction needed for Warner's questioning design and for which the probabilities p_{1k} for a "yes"- and p_{2k} for a "no"-answer are known, and question 2 on the sensitive membership of subgroup A . For example, the first question may be 'Is the number on your dice from 1 to 4?' or 'Is the birth date within

the interval from 1st of January to 19th of October?” or any other interval consisting of a certain subset of the possible outcomes. The information that the respondent actually has to provide in the crosswise version is whether the answers to both questions were the same (“then answer yes”) or not (“then answer no”). Yu et al. (2008) claim that “the interviewee does not face any sensitive questions” (p. 261f), although given the same result concerning the chosen randomization instruction, both implementations of Warner’s RR technique result in exactly the same answers (see the formal description of that fact in: Jann et al. 2012, p. 36) and have exactly the same theory (compare, Warner 1965, Sec. 2, and Yu et al. 2008, Sec. 3.2). However, results in the empirical study of Höglinger et al. (2014) suggest that respondents understand the instructions for use of the crosswise model approach better than of other RR techniques (p. 24).

Since Warner’s initial boost, various RR methods have been developed with the aim to increase the efficiency of the techniques. Horvitz et al. (1967) and Greenberg et al. (1969) substituted the second question of Warner’s original model by a question on membership of a completely non-sensitive group $B \subseteq U$ of a known size π_B unrelated to the membership of A . In the “forced RR questioning technique”, Boruch (1971) and Fidler and Kleinknecht (1977) substituted this question by the instructions just to say “yes”, or “no”. Moreover, the idea of the RR techniques has been successfully applied to categorical or quantitative variables (cf., for instance, the relevant standardizations in: Quatember 2015, ch. 6). Recently, Chaudhuri (2011), Chaudhuri and Christofides (2013), and Chaudhuri et al. (2016) wrote or edited books on the various aspects of the indirect questioning procedures. Their practical use in surveys on different sensitive subjects is well documented (see for instance, van den Hout et al. 2010; Krumpal 2012; Moshagen et al. 2012; Kirchner et al. 2013; De Hon 2014). Their effect on the data quality was also investigated in several studies with quite different results, which mainly underlines the sensitivity of such surveys to a great many aspects with the privacy protection of respondents among them (cf., for instance, Lensvelt-Mulders et al. 2005, 2006; Holbrook and Krosnick 2010; Coutts and Jann 2011; Jann et al. 2012; Wolter and Preisendörfer 2013; Höglinger et al. 2014; Höglinger and Diekmann 2017).

In order to have a chance of being recognized as an alternative to the common practice in the field, these techniques have not only to be simple in their application but also as general as possible in their theory. Hence, for the purpose of the estimation of π_A in a general probability sampling framework, the standardized theoretical approach of different RR questioning designs by Quatember (2009) incorporates the direct question on membership of group A , the question on membership of its complement A^C (Warner 1965), the question on membership of a completely non-sensitive group $B \subseteq U$ of a known size π_B unrelated to the membership of A (cf. Horvitz et al. 1967), as well as two other possible alternatives from the forced RR questioning technique with its instructions just to say “yes”, or “no” (cf. Boruch 1971) under a unified theoretical roof. Moreover, the possibility to assign different design probabilities to the sample members is added to this unified approach, enabling the conductors of the survey to tailor the privacy protection level offered by the design on individual level. This can be done according to a model concerning the different needs of each respondent or of subgroups of respondents (like the groups of men and women) following the principles of adaptive survey designs (cf. Schouten et al. 2018). In this extended standardized RR technique, respondent k is asked the direct question on membership of group A with an assigned design probability of p_{1k} ($0 < p_{1k} \leq 1$). Warner’s alternative question on membership of group A^C is given a probability of p_{2k} (with $p_{2k} < p_{1k}$ without loss of generality), and that of Horvitz et al. on membership of non-sensitive unrelated group B with relative size π_B one of p_{3k} . The instructions just to say “yes” or “no” have probabilities

of p_{4k} and p_{5k} ($0 \leq p_{ik} < 1$ for $i=2, 3, 4, 5$, and $\sum_{i=1}^5 p_{ik} = 1$). Note that this is clearly not an invitation to use all five questions/instructions in the same questioning design. Rather, the objective is to provide a unified theoretical framework that can be applied whenever one of all possible combinations of these questions or instructions is chosen. One can choose the design parameters p_{1k} to p_{5k} , and π_B according to one's own preferences and experiences with RR strategies, assumptions of the level of sensitivity of the variable under study [cf., for instance, the examples of Edgell et al. (1982, p. 95f), or in the Online Appendix of Höglinger and Diekmann (2017)], and models with respect to the level of privacy protection needed by respondent k . Furthermore, it does depend on the type of sensitivity of the subject under study which of the special cases of the standardized RR method by Quatember (2009) can statistically be most efficient for given levels of privacy protection (Sect. 4). In respect thereto, a dichotomous variable has to be classified according to the following categories: the variable is not sensitive at all; only the membership of subset A is sensitive, but not of A^C ; the membership of both population subsets is sensitive, but not equally; the membership of both subsets is equally sensitive.

Let the answer z_k of a sample unit k in the chosen RR design be

$$z_k = \begin{cases} 1, & \text{if sample unit } k \text{ answers "yes"} \\ 0, & \text{otherwise.} \end{cases}$$

Then, the term to be "imputed" into the HT estimator (2) instead of the unknown true y -value y_k of respondent k is

$$y_k^i = \frac{z_k - u_k}{v_k} \tag{4}$$

with $u_k \equiv p_{2k} + p_{3k} \cdot \pi_B + p_{4k}$ and $v_k \equiv p_{1k} - p_{2k}$ and has the expectation $E(y_k^i) = y_k$.

Proof

$$E(y_k^i) = \frac{E(z_k) - u_k}{v_k} = \frac{p_{1k}y_k + p_{2k}(1 - y_k) + p_{3k}\pi_B + p_{4k} - u_k}{v_k} = y_k$$

Presuming full cooperation as a reaction on the privacy protection offered by the RR questioning design and applying the HT-approach from (2), the estimator

$$\pi_{A,RR} = \frac{1}{N} \cdot \sum_s y_k^i \cdot d_k \tag{5}$$

is unbiased for parameter π_A for general probability sampling with design weights d_k under the given unified RR strategy.

For Warner's technique (and Yu et al.'s model) under SI sampling, estimator (5) results in the sample mean of the imputed values y_k^i with $u_k = p_{2k}$ and $v_k = p_{1k} - p_{2k}$, respectively. Furthermore, the unbiased estimator $\pi_{A,RR}$ (5) has a theoretical variance of

$$V(\pi_{A,RR}) = \frac{1}{N^2} \cdot \left(\sum_U \sum_U (\pi_{kl} - \pi_k \cdot \pi_l) \cdot \frac{y_k}{\pi_k} \cdot \frac{y_l}{\pi_l} + \sum_U \frac{u_k(1 - u_k)}{v_k^2} \cdot d_k + \sum_U y_k \cdot \frac{1 - v_k - 2u_k}{v_k} \cdot d_k \right) \tag{6}$$

□

Proof With E_{PS} , E_{RR} , and V_{PS} , V_{RR} denoting expectations and variances according to the probability sampling process PS and the RR design, $V(\pi_{A,RR})$ is divided into

$$V(\pi_{A,RR}) = V_{PS}(E_{RR}(\pi_{A,RR}|s)) + E_{PS}(V_{RR}(\pi_{A,RR}|s))$$

The first of the two summands from above yield the first of the three summands of Eq. (6). For the proof of the rest, we have to introduce the sample inclusion indicator $I_k = I\{k \in s\}$ with $E(I_k) = \pi_k$ (cf. Särndal et al. 1992, Sec. 2.4). For the covariance $C_{RR}(y_k^i, y_l^i|s) = 0$ applies for all units $k \neq l$. Therefore,

$$E_{PS}(V_{RR}(\pi_{A,RR}|s)) = E_{PS}\left(\frac{1}{N^2} \cdot V_{RR}\left(\sum_U y_k^i \cdot d_k \cdot I_k|s\right)\right) = \frac{1}{N^2} \cdot \sum_U V_{RR}(y_k^i) \cdot d_k$$

For $V_{RR}(y_k^i)$,

$$V_{RR}(y_k^i) = \frac{1}{v_k^2} \cdot V_{RR}(z_k)$$

applies. Then, $V_{RR}(z_k) = u_k + v_k \cdot y_k - (u_k + v_k \cdot y_k)^2 = u_k \cdot (1 - u_k) + v_k \cdot (1 - v_k - 2u_k) \cdot y_k$, which all together yields the result in Eq. (6).

For SI sampling, Warner’s method has a variance of

$$\frac{\pi_A(1 - \pi_A)}{n} \cdot \frac{N - n}{N - 1} + \frac{1}{Nn} \left(\sum_U \frac{p_{2k}(1 - p_{2k})}{(p_{1k} - p_{2k})^2} + \sum_U y_k \cdot \frac{1 - p_{1k} - p_{2k}}{p_{1k} - p_{2k}} \right).$$

□

3 Objectively calculated privacy protection versus accuracy

The aim of any indirect questioning design is the protection of the privacy of respondents in such a way that they become willing to respond truthfully even on questions of a rather sensitive matter. Of course, the effect of the applied technique on the respondents’ privacy protection has to be explained to the respondent in every necessary detail, so he or she is able to understand how their privacy is being protected. Höglinger et al. (2014) showed that the understanding of the technique’s principle correlates significantly with the development of trust in the strategy’s privacy protection, which is assumed to be a precondition to increase the willingness to cooperate (p. 25). For different indirect questioning designs, Coutts and Jann (2011) found proportions of respondents between 80 and 93 percent who felt they had completely understood the instructions (p. 178f). Hence, with respect to the quality of data, the effect of comprehensive training for the interviewers cannot be underestimated. The empirical results of Höglinger et al. (2014) also emphasized the role of the type of randomization instruction. They found that the percentage of respondents who felt that the used RR technique was cumbersome was slightly higher for procedures employing an explicit than an implicit randomization (p. 24).

As an example, considering again the crosswise model of Warner’s procedure, including an unrelated question bearing the randomization instruction with constant design parameters p_{1k} and p_{2k} for all survey units and the direct question on the sensitive attribute, explanations can be written down for use in postal or web surveys, or be

given orally by an interviewer in a face-to-face or telephone survey in the following manner: ‘The applied questioning technique will ensure that nobody will be able to link your response, may it be “yes” or “no”, with certainty directly to the sensitive question when you follow exactly the instructions below to keep your privacy safe: Don’t report the answers to the following two questions. Question 1: Think of a person (you, your mother, a friend,...), whose date of birth you know but without delivering this information to the interviewer and stick to it! Is the birth date within the interval from 1st of January to 19th of October? Question 2: Are you a member of subgroup A? Now, if your answers on both questions are the same, simply answer “yes”, and “no”, if they are not. A “yes”-answer of yours might then mean that the birth date, you were thinking of, is/is not within the given interval and you are/are not a member of group A. A “no”-answer might then mean that the birth date is/is not within the given interval and you are not/are a member of group A. Therefore, your privacy will be guaranteed.’

A measure of privacy protection should be considered to formally describe the dependency of the estimation efficiency on the level of privacy protection. For the particular family of RR techniques described in Sect. 2, for respondent k such a privacy protection measure with respect to a “yes”-answer ($z_k = 1$) may be given by

$$P_{1k} = \frac{\min[P(z_k = 1|k \in A), P(z_k = 1|k \in A^C)]}{\max[P(z_k = 1|k \in A), P(z_k = 1|k \in A^C)]} = \frac{u_k}{u_k + v_k}. \tag{7}$$

Regarding a “no”-answer ($z_k = 0$), the measure yields

$$P_{0k} = \frac{\min[P(z_k = 0|k \in A), P(z_k = 0|k \in A^C)]}{\max[P(z_k = 0|k \in A), P(z_k = 0|k \in A^C)]} = \frac{1 - u_k - v_k}{1 - u_k}. \tag{8}$$

On the one hand, the ratios P_{1k} and P_{0k} of two conditional probabilities equal to zero only when the privacy of respondent k with respect to a “yes”- or “no”-answer is not protected at all by the questioning design. This applies at the same time for both measures only in the case of the direct questioning model, in which, for example, $P(z_k = 1|k \in A) = 1$ and $P(z_k = 1|k \in A^C) = 0$ applies. On the other hand, the privacy protection measures P_{1k} and P_{0k} reach the maximum values of one, when privacy is totally protected with regard to the specific answer z_k , meaning that the given answer bares absolutely no information on the true value y_k of the unit. Warner’s method respectively its practical implementation by Yu et al. (2008) yield $P_{1k} = p_{2k}/p_{1k}$ and $P_{0k} = (1 - p_{1k})/(1 - p_{2k})$. This means that both possible answers are equally protected. Other methods like the unrelated question approach of Horvitz et al. (1967) and the forced method of Boruch (1971) are able to protect both possible answers differently (Quatember 2009, Sec. 4). But in these cases, where Warner’s possible second question on membership of the complementary group is substituted by an unrelated nonsensitive question or the instructions just to say “yes” or “no” regardless of the membership of group A, a possible self-protective “no”-answer is introduced into the questioning design giving the respondent the opportunity to be “on the save side” if the membership of the complementary group A^C is not as sensitive as the membership of A itself. In empirical studies, a considerable answer bias was observed in applications of the forced RR technique (Edgell et al. 1982, p. 97, or Coutts and Jann 2011, p. 183). For all these reasons, the implementation of Warner’s original technique by Yu et al. (2008) seems to set the standard.

Assuming an approximately uniform distribution of birth days in the population, for the standardized RR questioning design with the randomization instruction from above ('1st of January to 19th of October') with $p_{1k} \approx 292/365 = 0.8$, $p_{2k} \approx 73/365 = 0.2$, and $p_{3k} = p_{4k} = p_{5k} = 0$ for all survey units, the measures in Eqs. (7) and (8) result both in 0.25, thus protecting both possible answers equally for all survey units. In a specific experiment, Fidler and Kleinknecht (1977) showed for variables of very different levels of sensitivity that their choice of the design parameters for the forced RR strategy produced nearly full and truthful response for all of them (ibid., p. 1048). Calculating Eqs. (7) and (8) with their choices of the design probabilities yields privacy protection values P_{1k} and P_{0k} of 0.231. This corresponds to the main results that can be derived from the experiment by Soeken and Macready (1982) and to recommendations given already by Greenberg et al. (1969). In accordance with these findings, choosing P_{1k} and P_{0k} close to a value of 0.25 seems to be a good practice for most variables to avoid refusals and untruthful answering of respondents in a survey with randomized responses.

In the brackets of (6), the first summand is the variance (3) of the HT estimator $\pi_{A,HT}$ under full response. This means that the expression

$$C \equiv \frac{1}{N^2} \cdot \left(\sum_U \frac{u_k(1-u_k)}{v_k^2} \cdot d_k + \sum_U y_k \cdot \frac{1-v_k-2u_k}{v_k} \cdot d_k \right) \tag{9}$$

may be considered as the costs C to be paid by the data analyst for the higher privacy protection of the respondents with regard to decreasing accuracy, which in turn will pay off in terms of higher response and truthful answering rates. For the crosswise model and Warner's technique under SI sampling, the costs C result in

$$\frac{1}{Nn} \cdot \left(\sum_U \frac{p_{2k}(1-p_{2k})}{(p_{1k}-p_{2k})^2} + \sum_U y_k \cdot \frac{1-p_{1k}-p_{2k}}{p_{1k}-p_{2k}} \right).$$

The costs C can be directly expressed by the privacy protection measures P_{1k} and P_{0k} to show the direct dependency of the variance of the general estimator $\pi_{A,RR}$ on the privacy protection offered by a questioning design. From Eqs. (7) and (8), the terms v_k and u_k can be expressed by

$$v_k = \frac{(1-P_{1k})(1-P_{0k})}{1-P_{1k}P_{0k}}$$

and

$$u_k = \frac{P_{1k}(1-P_{0k})}{1-P_{1k}P_{0k}}$$

($P_{1k}, P_{0k} \neq 1$). Eventually, inserting these expressions for u_k and v_k into Eq. (9), the term C can be expressed by

$$C = \frac{1}{N^2} \cdot \left(\sum_{U \cap A} \frac{P_{0k}}{(1-P_{1k})(1-P_{0k})} \cdot d_k + \sum_{U \cap A^c} \frac{P_{1k}}{(1-P_{1k})(1-P_{0k})} \cdot d_k \right) \tag{10}$$

with the set $U \cap A$ consisting of the population elements of U belonging to subset A , and set $U \cap A^c$ consisting of the population elements belonging to the complementary group A^c .

Equation (10) shows that under the assumption of full cooperation, the efficiency of this unified RR strategy depends solely on the privacy protection offered by the questioning design. Actually, the additional costs C are a linear function of the privacy protection provided by the questioning design on individual level, when measured by P_{1k} and P_{0k} from Eqs. (7) and (8).

4 Subjectively perceived privacy protection versus response propensity

Chaudhuri and Christofides (2013) mentioned that “common sense mandates that the perceived protection of privacy is crucial in deciding to participate in a survey dealing with sensitive issues. In fact, it is gaining ground the opinion that the perception of privacy protection should also be considered when the protection of privacy offered by various indirect questioning techniques is examined” (ibid., p. 169). Clearly, the privacy protection objectively measured may differ from the privacy protection subjectively perceived by the individuals to be surveyed. While the subjective privacy protection seems to be the crucial point for the willingness to cooperate, the objective protection of privacy is essential for the accuracy of the survey estimates as shown in Sect. 3.

While, for instance, the majority of respondents will possibly be able to correctly assess the design probabilities provided by a randomization instruction that makes use of only one dice, one coin, one deck of cards, or a spinner, this might not be the case if, for example, two or more dice are involved. Let’s think of three dice as an example. To allow the design probabilities for the crosswise-version of Warner’s model again to be close to $p_{1k}=0.8$, and $p_{2k}=0.2$ for all survey units, question 1 may ask, whether the total of the three thrown dice is an element of the set $\{8, 9, 10, 11, 12, 13, 14, 15, 17\}$. The probability p_{1k} that a respondent provides with his or her actual process reply the answer to the question on membership of subpopulation A is given by $174/216 = 0.805$, whereas the probability p_{2k} that he or she provides the answer to the question on membership of A^C is $42/216 = 0.194$. According to Eqs. (7) and (8), this yields the following measures of objective privacy protection: $P_{1k}=P_{0k}=0.241$.

When, although the randomization instructions are explained sufficiently, a respondent k would derive the probability that he or she has actually to deliver the answer on the direct question on membership of A within the crosswise model by observing that only 9 of the 16 possible outcomes from 3 to 18 for the total of the three dice are elements of the set $\{8, 9, 10, 11, 12, 13, 14, 15, 17\}$ and the probability for an answer on the direct question on membership of A^C by the fact that the remaining 7 possible outcomes are elements of the complementary set of possible numbers, such a respondent might erroneously think that the design parameters might be given by the following “perceived probabilities”: $pp_{1k} \approx 9/16 = 0.5625 < 0.805 = p_{1k}$ and $pp_{2k} \approx 7/16 = 0.4375 > 0.194 = p_{2k}$. Hence, even when such a respondent does not think of exact these probabilities, at least he or she might feel that the questioning design protects his or her privacy more than it really does because of an underestimation of the probability p_{1k} .

Using the same approach that was used in measures Eqs. (7) and (8) for the calculations of the objective privacy protection with regard to the answers “yes” or “no”, but applying therein the perceived design probabilities pp_{ik} instead of the correct probabilities p_{ik} ($i=1, 2$), for such a sample element k , the subjectively perceived privacy protection PP_{1k} regarding a “yes”-answer may be calculated by

$$PP_{1k} = \frac{u'_k}{u'_k + v'_k} \quad (11)$$

with $u'_k \equiv pp_{2k} + pp_{3k} \cdot \pi_B + pp_{4k}$ and $v'_k \equiv pp_{1k} - pp_{2k}$. With respect to a “no”-answer, this yields a subjective privacy protection measure of

$$PP_{0k} = \frac{1 - u'_k - v'_k}{1 - u'_k}. \tag{12}$$

With the perceived design probabilities $pp_{1k}=0.5625$, $pp_{2k}=0.4375$, this yields $PP_{1k} = PP_{0k} = 0.4375/0.5625 = 0.7 > 0.241 = P_{1k} = P_{0k}$. The measures of the perceived privacy protection are more than three times the measures P_{1k} and P_{0k} of the true privacy protection. This means that in this case, respondent k should have a higher response propensity compared to a respondent who thinks with the correct design probabilities.

When question 1 of the crosswise version of Warner’s model asks, for example, whether the total of three dice equals an element of the set $\{3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 18\}$ or not, the true probability p_{1k} is again $0.80\dot{5}$ for all sample units k , but the set contains five elements more than $\{8, 9, 10, 11, 12, 13, 14, 15, 17\}$ from the previous example. For a respondent k , not understanding the true effect of the explicit randomization instruction with regard to the design probabilities, this might mean $pp_{1k} \approx 14/16 = 0.875 > 0.80\dot{5} = p_{1k}$ and $pp_{2k} \approx 2/16 = 0.125 < 0.19\dot{4} = p_{2k}$. Hence, the randomization instruction might also work in the opposite direction, when a respondent perceives a lower privacy protection with the randomization instruction compared to the real one: $PP_{1k} = PP_{0k} = 0.125/0.875 = 0.143 < 0.241 = P_{1k} = P_{0k}$.

For every respondent k , the differences of the privacy protection as subjectively perceived and objectively given for both possible answers can be formalized by

$$\Delta_{1k} = PP_{1k} - P_{1k} \tag{13}$$

and

$$\Delta_{0k} = PP_{0k} - P_{0k}. \tag{14}$$

In the two examples of possible perceived privacy protection from above, a respondent k , who derives incorrect design probabilities pp_{1k} and pp_{0k} , measures (13) and (14) result in $+0.536$ and -0.099 , respectively. Assuming that the objective measures P_{1k} and P_{0k} were reasonably fixed according to own preferences or recommendations from previous studies as already mentioned to allow maximum cooperation and high estimation efficiency, the measures Δ_{1k} and Δ_{0k} must not be negative for all $k \in s$.

For the comparatively uncomplicated practical method to assign the design probabilities to the different questions or instructions of the standardized RR strategy by using different intervals of birth dates, the subjectively perceived privacy protection PP_{1k} and PP_{0k} in Eqs. (11) and (12) might correspond to the objectively measured privacy protection P_{1k} and P_{0k} in Eqs. (7) and (8) yielding $\Delta_{1k} = \Delta_{0k} = 0$ in Eqs. (13) and (14). This might always be the case when the true distribution of the possible outcomes of the randomization device is (at least: approximately) uniformly distributed as it is the case also for one dice. However, Höglinger and Diekmann (2017) found in their study that even some of the “birth date”-questions used might have been problematic either because they left too much space to respondents in selecting the person, or some of the respondents simply did not know the answer regarding the birth date of a certain person (p. 10 of the Online Appendix). This problem can be avoided by starting the instruction with ‘Think of a person, whose date of birth you know and stick to it.’

Although it could be found ethically problematic, some authors recommended taking advantage of such possible lack of understanding regarding the effect of the randomization

device on the level of privacy protection offered by an RR strategy. For instance, Lensvelt-Mulders et al. (2005) noted that "... an extra advantage of using the forced response method is that the perceived protection of the respondents can be manipulated. It is a well-known fact that people have incorrect intuitions about the calculation of probabilities. This flaw can be used to the advantage of researchers by making the subjective privacy protection larger than the true statistical privacy protection (ibid., p. 263)."

In this respect, a mathematically more sophisticated randomizing instruction with no uniform distribution that also requires no explicit instrument was suggested by Diekmann (2012) and makes use of the so-called "Newcomb-Benford distribution" (cf. Newcomb 1881), which is also applied in detecting fraud in accounting data or scientific publications (cf., for instance, Durtschi et al. 2004; Diekmann 2007). In the crosswise version of Warner's RR questioning design, the respondent may be asked to think of a person of whom he or she recalls, for instance, the house number. The second question unrelated to the one on membership of group A is, whether the first digit of the house number is an element of the set $\{1, 2, 3, 4, 8, 9\}$ or not [see the application example in: Höglinger et al. (2014, p. 14)].

Diekmann (2012) emphasized that for this randomization instruction there is a discrepancy between the design probabilities as perceived by the respondents and the correct probabilities. Contrary to the intuition of most of the respondents, the probability of the first digit does not follow the uniform distribution but follows approximately the Newcomb-Benford distribution (Diekmann 2012, pp. 329 and 332). Hence, with the instructions given above, the true probability p_{1k} of a "yes"-answer to that question is about 0.796. The measures P_{1k} and P_{0k} result in 0.256 for all units $k \in s$. The perceived probability pp_{1k} of picking a house number with the first digit within the set $\{1, 2, 3, 4, 8, 9\}$ might be around $pp_{1k} = 6/9 = 0.6$ and not 0.796. This "illusion" (ibid., p. 330) should have a positive effect on the perceived privacy protection with regard to the questioning design. According to Eqs. (11) and (12), the wrong assumption of a uniform distribution of the first digit would result in perceived privacy protection measures of $0.3/0.6 = 0.5$ instead of 0.256 for both PP_{1k} and PP_{0k} and Δ_{1k} and Δ_{0k} both being considerably larger than zero. Hence, the actual protection of privacy offered by the design would be substantially overestimated. This should increase the willingness to cooperate of respondents not understanding the true effect of the RR device. It is up to the data collector to balance between the ethical issues and the desire for efficient parameter estimation.

One design feature of the crosswise model that might further increase the subjective perception of privacy protection is that the respondents are not explicitly asked to provide the answer on membership of group A or the complementary group A^C as in Warner's original questioning design, although these answers are actually exactly what they have to deliver. This might further enlarge the measures Δ_{1k} and Δ_{0k} for this implementation of the Warner model. In the empirical study by Höglinger et al. (2014), about two-thirds of nearly 1000 test persons using the crosswise model with an implicit randomization instruction answered "yes, definitely" or at least "rather yes" on the question "What is your personal opinion: Does the special survey technique provide 100% protection of your answers to the sensitive questions? (p. 44)". This means that a part of these respondents was convinced that the applied crosswise model protected their answers perfectly. Actually, this would only be true, if the measures of privacy protection, P_{1k} and P_{0k} , would equal 1. In the cited study, the design probabilities of the crosswise model were varied moderately among respondents by the use of different intervals in the birth date-question yielding to different values of the objective privacy protection measures from 0.2 to 0.351 (p. 30f), thus far away from 1. For this group of "believers", the formalization of the subjectively perceived privacy protection according to Eqs. (11) and (12) provides measures of $PP_{1k} = PP_{0k} = 1$

and the differences Δ_{1k} and Δ_{0k} reach their possible maxima. Further, a high percentage of 97% of the respondents believed that they applied the technique “rather” or definitely” correct, which is also of great importance with respect to data quality (p. 44).

A further feature of an RR procedure that might affect the individuals’ perceived privacy protection positively in the discussed manner is its extension to two (or even more) stages (cf. for instance, Mangat and Singh 1990): At stage I of a two-stage RR questioning design, a sampling unit k is asked with probability p_{1k}^I the direct question on the sensitive membership of group A. With the remaining probability, the unit is directed to stage II, where, for instance, a special case of the standardized RR questioning design from Sect. 2 is applied with design parameters p_{1k}^{II} to p_{5k}^{II} and π_B . Quatember (2012) proved theoretically that in contrast to what was claimed in some publications in the past, multistage RR questioning designs cannot perform better in terms of their theoretical variances than their one-stage basic versions, when the respondents’ objective privacy protection, being measured by Eqs. (7) and (8), is also taken into consideration. In other words, to achieve a higher efficiency for the estimates, the level of objective privacy protection has to be lower for a certain RR questioning design whether or not it is applied at one or more stages.

However, although the objective privacy protection is equal for one- or two-stage designs, for respondent k , the differences Δ_{1k} and Δ_{0k} from Eqs. (13) and (14) might be larger than zero for the two-stage designs in cases where the probability p_{1k}^{II} of being asked the sensitive question at the second process stage is low compared to this design probability p_{1k} of the one-stage version of the same questioning design. In practice though, even the addition of only a second design stage might become counterproductive because the cooperation rate might further decrease due to the higher complexity of the questioning process yielding an increase of respondents’ burden when compared, for example, to the simple crosswise model.

5 Conclusion

If the direct questioning on the sensitive variable leads to non-ignorable nonresponse and untruthful answers, as very often expected in statistical surveys particularly on sensitive subjects, a considerably biased estimator might be the consequence. For such cases, the higher complexity of the indirect questioning designs might pay off assuming an increase of respondents’ cooperation. Consequently, the accuracy of the estimator increases although its variance exceeds the theoretical variance of the direct questioning. It is evident that the overall performance of the exemplarily discussed standardized RR strategy for the estimation of proportions of sensitive behaviour in terms of estimation accuracy and avoidance of nonresponse and untruthful answering is a function of the level of privacy it offers to the respondents, which can be considered from the points of view of an objectively measurable and a subjectively perceived protection. On the one hand, for this family of RR strategies it is proven that the privacy protection objectively offered by a questioning design directly affects the efficiency of the estimator as shown in Eq. (10). On the other hand, it seems quite comprehensible that the higher the subjective level of privacy protection is, the higher the respondents’ willingness to cooperate will be. That is what indirect questioning designs are all about. Therefore, one has to pay attention to this fact, when choosing adequate randomization instructions for the application of an RR technique. Therefore, the best practice would be to avoid that the subjectively perceived privacy protection is less than the privacy protection actually connected with the questioning design, which is

expressed by claiming that Δ_{1k} and Δ_{0k} from Eqs. (13) and (14), measuring the amount of the wrong reception of the offered privacy protection, must not be negative.

Acknowledgements Open access funding provided by Johannes Kepler University Linz.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- Boruch, R.F.: Assuring confidentiality of responses in social research: a note on strategies. *Am. Sociol.* **6**, 308–311 (1971)
- Boruch, R.F.: Relations among statistical methods for assuring confidentiality of social research data. *Soc. Sci. Res.* **1**, 403–414 (1972)
- Chaudhuri, A.: *Randomized Response and Indirect Questioning Techniques in Surveys*. CRC Press, Boca Raton (2011)
- Chaudhuri, A., Christofides, T.C.: *Indirect Questioning in Sample Surveys*. Springer, Heidelberg (2013)
- Chaudhuri, A., Christofides, T.C., Rao, C.R. (eds.): *Handbook of Statistics (Volume 34): Data Gathering, Analysis and Protection of Privacy through Randomized Response Techniques: Qualitative and Quantitative Human Traits*. Elsevier, Amsterdam (2016)
- Coutts, E., Jann, B.: Sensitive questions in online surveys: experimental results for the randomized response technique (RRT) and the unmatched count technique (UCT). *Sociol. Methods Res.* **40**(1), 169–193 (2011)
- De Hon, D.: *De Nederlandse topsporter en het anti-dopingbeleid 2014–2015*. Doping Autoriteit (2015). http://www.dopingautoriteit.nl/media/files/2015/Topsportonderzoek_doping_2015-07-21_DEF.pdf. Accessed 21 Mar 2018
- Diekmann, A.: Not the first digit! Using Benford's Law to detect fraudulent scientific data. *J. Appl. Stat.* **34**(3), 321–329 (2007)
- Diekmann, A.: Making use of "Benford's Law" for the randomized response technique. *Sociol. Methods Res.* **41**(2), 325–334 (2012)
- Durtschi, C., Hillison, W., Pacini, C.: The effective use of Benford's Law to assist in detecting fraud in accounting data. *J. Forensic Account.* **V**, 17–34 (2004)
- Edgell, S.E., Himmelfarb, S., Duchan, K.L.: Validity of forced responses in a randomized response model. *Sociol. Methods Res.* **11**(1), 89–100 (1982)
- Fidler, D.S., Kleinknecht, R.E.: Randomized response versus direct questioning: two data collection methods for sensitive information. *Psychol. Bull.* **84**(5), 1045–1049 (1977)
- Greenberg, B.G., Abul-Elä, A.-L.A., Simmons, W.R., Horvitz, D.G.: The unrelated question randomized response model: theoretical framework. *Journal of the American Statistical Association* **64**(326), 520–539 (1969)
- Groves, R.M., Fowler, F.J., Couper, M.P., Lepkowski, G.M., Singer, E., Tourangeau, R.: *Survey Methodology*. Wiley, Hoboken (2004)
- Höglinger, M., Diekmann, A.: Uncovering a blind spot in sensitive question research: false positives undermine the crosswise-model RRT. *Polit. Anal.* **25**, 131–137 (2017). <https://doi.org/10.1017/pan.2016.5>. Accessed 21 Mar 2018
- Höglinger, M., Jann, B., Diekmann, A.: Sensitive questions in online surveys: an experimental evaluation of the randomized response technique and the crosswise model. University of Berne Social Sciences Working Paper No. 9 (2014)
- Holbrook, A.L., Krosnick, J.A.: Measuring voter turnout by using the randomized response technique. *Public Opin. Q.* **74**(2), 328–343 (2010)
- Horvitz, D.G., Shah, B.V., Simmons, W.R.: The unrelated question randomized response model. In: *Proceedings of the Section on Survey Research Methods, American Statistical Association*, pp. 65–72 (1967)
- Jann, B., Jerke, J., Krumpal, I.: Asking sensitive questions using the crosswise model: an experimental survey measuring plagiarism. *Public Opin. Q.* **76**(1), 32–49 (2012)

- Kirchner, A., Krumpal, I., Trappmann, M., von Hermann, H.: Messung und Erklärung von Schwarzarbeit in Deutschland—Eine empirische Befragungsstudie unter besonderer Berücksichtigung des Problems der sozialen Erwünschtheit (Measuring and explaining undeclared work in Germany—an empirical survey with a special focus on social desirability bias). *Zeitschrift für Soziologie* **42**(4), 291–314 (2013). **(in German)**
- Krumpal, I.: Estimating the prevalence of xenophobia and anti-Semitism in Germany: a comparison of randomized response and direct questioning. *Soc. Sci. Res.* **41**(6), 1387–1403 (2012)
- Lensvelt-Mulders, G.J.L.M., Hox, J.J., van der Heijden, P.G.M.: How to improve the efficiency of randomized response designs. *Qual. Quant.* **39**, 253–265 (2005)
- Lensvelt-Mulders, G.J.L.M., van der Heijden, P.G.M., Laudy, O., van Gils, G.: A validation of a computer-assisted randomized response survey to estimate the prevalence of fraud in social security. *J. R. Stat. Soc. A* **169**(2), 305–318 (2006)
- Lohr, S.: *Sampling: Design and Analysis*, 2nd edn. Brooks/Cole, Boston (2010)
- Mangat, N.S., Singh, R.: An alternative randomized response procedure. *Biometrika* **77**, 439–442 (1990)
- Moshagen, M., Musch, J., Erdfelder, E.: A stochastic lie detector. *Behav. Res.* **44**, 222–231 (2012)
- Newcomb, S.: Note on the frequency of use of the different digits in natural numbers. *Am. J. Math.* **4**, 39–40 (1881)
- Quatember, A.: A standardization of randomized response strategies. *Surv. Methodol.* **35**(2), 143–152 (2009)
- Quatember, A.: An extension of the standardized randomized response technique to a multi-stage setup. *Stat. Methods Appl.* **21**(4), 475–484 (2012)
- Quatember, A.: *Pseudo-populations. A Basic Concept in Statistical Surveys*. Springer, Cham (2015)
- Särndal, C.-E., Swensson, B., Wretman, J.: *Model-Assisted Survey Sampling*. Springer, New York (1992)
- Schouten, B., Peytchev, A., Wagner, J.: *Adaptive Survey Design*. CRC Press, Boca Raton (2018)
- Soeken, K.L., Macready, G.B.: Respondents' perceived protection when using randomized response. *Psychol. Bull.* **92**(2), 487–489 (1982)
- Van den Hout, A., Böckenholt, U., van der Heijden, P.G.M.: Estimating the prevalence of sensitive behaviour and cheating with a dual design for direct questioning and randomized response. *Appl. Stat.* **59**(4), 723–736 (2010)
- Warner, S.L.: Randomized response: a survey technique for eliminating evasive answer bias. *J. Am. Stat. Assoc.* **60**, 63–69 (1965)
- Wolter, F., Preisendörfer, P.: Asking sensitive questions: an evaluation of the randomized response technique versus direct questioning using individual validation data. *Sociol. Methods Res.* **42**(3), 321–353 (2013)
- Yu, J.-W., Tian, G.-L., Tang, M.-L.: Two new models for survey sampling with sensitive characteristic: design and analysis. *Metrika* **67**, 251–263 (2008)